NOKIA

5620 SAM
SERVICE AWARE MANAGER

ALARM REFERENCE

3HE-10681-AAAL-TQZZA

Issue 2

July 2020

Legal notice

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2020 Nokia.

Conformance statements

See the Alcatel-Lucent Content Standards (http://ndoc.all.alcatel-lucent.com/toolbox/standards/style/content.shtml) for details on the content to include in this block.

Contents

About this document **10**

1 Overview **11**

1.1 Alarm information **11**

1.2 NE-specific alarm information **12**

1.3 Alarm information in other formats **14**

1.4 OSS alarm monitoring **14**

1.5 New alarms by 5620 SAM release **14**

2 1830 PSS (PSS-36 OCS, PSS-64 OCS) 89
2.1 Alarms **89**

3 1830 PSS (PSS-4, PSS-8, 16/32) 197
3.1 Alarms **197**

4 1830 VWM OSU 767
4.1 Alarms **767**

5 7210 SAS-D 811
5.1 Alarms **811**

6 7210 SAS-E 869
6.1 Alarms **869**

7 7210 SAS-K 921
7.1 Alarms **921**

8 7210 SAS-M 981
8.1 Alarms **981**

9 7210 SAS-Mxp 1069
9.1 Alarms **1069**

10 7210 SAS-R 1141
10.1 Alarms **1141**

11 7210 SAS-Sx 1217
11.1 Alarms **1217**

12 7210 SAS-T 1285
12.1 Alarms **1285**

13 7210 SAS-X 1363
13.1 Alarms **1363**

14 7450 ESS 1445
14.1 Alarms **1445**

15 7701 CPAA 1635
15.1 Alarms **1635**

16 7705 SAR 1677
16.1 Alarms **1677**

17 7705 SAR-H 1805

17.1 Alarms 1805

18 7710 SR **1913**
18.1 Alarms **1913**
19 7750 SR **2025**
19.1 Alarms **2025**
20 7750 SR MG **2227**
20.1 Alarms **2227**
21 7950 XRS **2391**
21.1 Alarms **2391**
22 8000 MDR **2557**
22.1 Alarms **2557**
23 936x/996x SC access point **2581**
23.1 Alarms **2581**
24 9471 WMM **2733**
24.1 Alarms **2733**
25 9500 MPR **2881**
25.1 Alarms **2881**
26 9500 MPRe **2991**
26.1 Alarms **2991**
27 9774 LMG **3043**
27.1 Alarms **3043**
28 9966 SC GW **4009**
28.1 Alarms **4009**
29 9xxx eNodeB **4197**
29.1 Alarms **4197**
30 Cloud Mobility Manager **4831**
30.1 Alarms **4831**
31 7850 VSG **4909**
31.1 Alarms **4909**
32 DC VSA-8 ..... **5011**
32.1 Alarms **5011**
33 VSC **5087**

33.1 Alarms 5087

34 DSC **5167**
34.1 Alarms **5167**
35 FlexiPacket MultiRadio **5191**
35.1 Alarms **5191**
36 Generic NE **5207**
36.1 Alarms **5207**
37 HIP **5249**
37.1 Alarms **5249**
38 FlexiPacket Hub 800 ..... **5275**
38.1 Alarms **5275**
39 Unspecified NE **5299**
39.1 Alarms **5299**
40 Nokia - FDD Airscale **5681**
40.1 Alarms **5681**
41 LTE OMS **5749**
41.1 Alarms **5749**
42 OpenFlow **5871**
42.1 Alarms **5871**
43 OS10K **5885**
43.1 Alarms **5885**
44 OS6250 ..... **5933**
44.1 Alarms **5933**
45 OS6400 ..... **5985**
45.1 Alarms **5985**
46 OS6450 ..... **6027**
46.1 Alarms **6027**
47 OS6850/6850E **6075**
47.1 Alarms **6075**
48 OS6855 ..... **6127**
48.1 Alarms **6127**
49 OS6860/OS6860E **6173**

49.1 Alarms 6173
50 OS6900 6219
50.1 Alarms 6219
51 OS9600 6275
51.1 Alarms 6275
52 OS9700 6317
52.1 Alarms 6317
53 OS9700E/9800E 6359
53.1 Alarms 6359
54 OS9800 6411
54.1 Alarms 6411

About this document

Purpose

The *5620 SAM Alarm Reference* describes the alarms that the 5620 SAM can raise against managed NEs, network objects, and platform components. The alarms are organized into chapters by NE type, and each alarm is presented in tabular format. Alarms that apply to multiple NE types have multiple entries in this document; the only difference in the tables for these alarms is the applicable major NE release information.

See the *5620 SAM Troubleshooting Guide* for information about using alarms to troubleshoot the managed network. See the *5620 SAM User Guide* for information about alarm support, policies, and management using the 5620 SAM.

Document support

Customer documentation and product support URLs:

- Customer Documentation Welcome Page
- Technical support

How to comment

Documentation feedback

1 Overview

1.1 Alarm information

Alarm entry structure

Table 1-1, “EquipmentDegraded” (p. 11) contains a sample alarm entry.

Table 1-1 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm (3) Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure (450)	Release: • 5.0.0 • 6.0.0 • 7.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

The table title for an alarm entry is the alarm name. When the same alarm name is found in multiple packages, the table title includes the package name in parentheses. Each alarm entry contains the following information:

Alarm fields

- Name—the alarm name, and the alarm name ID in parentheses
- Type—the alarm type, and the type ID in parentheses
- Package—the containing package of the alarm, which maps to a package in the *5620 SAM-O XML Reference*
- Raised on class—the package and object class in package.class format
- Severity—the alarm default severity level
- Specific problem—the user-friendly alarm name (applicable to RAN NEs only)
- Implicitly cleared—whether the alarm automatically clears when the clearing alarm condition is true
- Default probable cause—the typical probable cause of the alarm, and the probable cause ID in parentheses
- Applicable major NE releases—the major device releases against which the alarm can be raised; the releases are applicable to the device specified in the chapter title
- Description—the alarm description

- Raising condition—a logic statement that describes the internal 5620 SAM parameter values that initiate the raising of the alarm
- Clearing condition—a logic statement that describes the internal 5620 SAM parameter values that initiate the clearing of the alarm
- Remedial action—a statement or series of steps recommended as the fault clearance procedure for the alarm

1.2 NE-specific alarm information

Unspecified NE alarms

Unspecified NE alarms are alarms that are not yet directly associated with one or more NE types.

Note: Associating alarms with specific NE types is an ongoing effort. For NE-specific information about an unspecified NE alarm, contact technical support.

5620 SAM platform alarms

5620 SAM platform alarms are alarms that the 5620 SAM raises in response to a condition in the 5620 SAM system that is not associated with an NE, for example, a database fault or the crossing of a disk-capacity threshold.

9471 WMM alarms

The 9471 WMM is based on a platform that supports many different applications. Some of the alarms that are described in this document apply to platform functions that the 9471 WMM does not utilize. Therefore, the 5620 SAM does not raise some of the 9471 WMM alarms listed in this document.

Some 9471 WMM alarm attributes are dynamic and are populated at runtime. Due to their dynamic nature, the following 9471 WMM alarm attributes are assigned generic values in this document:

- severity
- probable cause
- alarm type

Note: 9471 WMM alarms are provided in this document as a courtesy to assist in alarm identification and mapping. The *9471 Wireless Mobility Manager (MME) Alarm Dictionary 418-111-208* is the primary source for 9471 WMM alarm information.

eNodeB alarms and events

The eNodeB supports the following notification types:

- Alarms-fault notifications that are assigned one of the standard severity levels. Alarms are displayed in the alarms window and the Faults tab of NE and object properties forms.
- Events-notifications or warnings about specific NE actions. Events are displayed in the Events Log tab of the ENB Equipment properties form on a per-NE basis.

Each alarm that originates from an eNodeB is named with an InfoKey ID. An alarm that the 5620 SAM raises in response to network conditions that involve an eNodeB is named using the standard format.

See the *9412 eNodeB Alarms and Events Reference Guide* for more information about eNodeB alarms and events, including impact to network operation.

Specific problem for eNodeB and 9774 LMG alarms

The user-friendly name of eNodeB and 9774 LMG InfoKey alarms and events is represented by the "specific problem" field in the 5620 SAM alarm schema.

ADAC alarms

eNodeB alarms that are defined with Alarm Nature = ADAC (auto.) are shown in 5620 SAM GUI as Implicitly cleared = "true" and are represented in the 9400 NEM with Alarm Nature = ADAC ().

eNodeB software upgrade alarms

The 5620 SAM raises the NodeUpgraded info alarm when a managed eNodeB successfully undergoes an upgrade to a major software release, such as from LA6.0 to LR13.1.L. The 5620 SAM does not raise the alarm for software updates to maintenance releases or corrective loads within a major release, such as from LR13.1.L to LR13.1.L CL1.

Applicable classes for eNodeB releases

The “Raised on classes” information for an eNodeB alarm can vary between the applicable major NE releases. Alarm class applicability in this document is presented generically without specifying variations per release.

9500 MPR alarms

See *9500 MPR Maintenance and Trouble Clearing* for a listing of detailed remedial action procedures for 9500 MPR alarms.

1830 PSS alarms

See the *1830 PSS Maintenance and Trouble-clearing User Guide* for a listing of detailed remedial action procedures for 1830 PSS alarms.

External EMS alarms

Alarms that originate from external EMS that the 5620 SAM can manage, such as the 9959 NPO, are often dynamic and can be customized by users. The 5620 SAM has no information about an external EMS alarm until the alarm is sent to the 5620 SAM. Therefore, external EMS alarms are not described in this document. See the documentation of the relevant EMS for more information about the alarms that it can send to the 5620 SAM.

1.3 Alarm information in other formats

Alarm information in other formats

The alarm information in this document is also available in CSV and XML formats. You can use the alarmDetails.csv and alarmDetails.xml alarm reference files to tailor the alarm information to your requirements. For example, you can compare the files to determine what alarm information changes between 5620 SAM releases. Contact your support representative for more information.

1.4 OSS alarm monitoring

OSS alarm monitoring

See the *5620 SAM XML OSS Interface Developer Guide* for information about managing alarms using a 5620 SAM OSS client.

1.5 New alarms by 5620 SAM release

Introduction

This section lists the new alarms for each 5620 SAM release by alarm name and alarm ID. Consider the following statements when reviewing the information in this section:

- The alarm name identifies an alarm in the 5620 SAM GUI. The alarm ID identifies an alarm over OSSI.
- Alarm IDs are unique. When an alarm is no longer supported by the 5620 SAM, the alarm ID is not reused by a new alarm.
- If an alarm is renamed, it is typically assigned a new alarm ID. Therefore, renamed alarms can be listed in this section as new. These alarms existed under different alarm names and alarm IDs in previous releases of the 5620 SAM.

For more information about the alarms listed in this section, see the relevant alarm information tables in the NE-specific chapters of this document.

Maintenance releases

Some maintenance releases may not be listed in this section because no new alarms were added.

New alarms for 5620 SAM Release 14.0 R10

Alarm name	Alarm ID
Application4G_massNBHeNbOutOfService	12737
Application4G_nbHeNbOutOfService	12738
BSR_pwdLoginFailure	12739
BSR_pwdNokiaSupportAccountOperationFailure	12740

BSR_pwdServiceProviderAccountOperationFailure	12741
FGW_bsrDataFileEntryInvalid	12742
FemtoUpgradeRulesFileAlarm	12743
NBIoTLTECell_lteNbIotRrcSctpAssociationFailure	12744
NBIoTLTECell_spareNbIotCellAlarm1	12745
NBIoTLTECell_spareNbIotCellAlarm2	12746
NBIoTLTECell_spareNbIotCellAlarm3	12747
OAM_NBIoTLTECellDown	12748

New alarms for 5620 SAM Release 14.0 R9

Alarm name	Alarm ID
ActivationSessionAutoClosed	12372
Application4G_spareAlarmApplication4G1	12394
Application4G_spareAlarmApplication4G2	12395
Application4G_spareAlarmApplication4G3	12396
BSR_downloadSwDiffThanTargetSw	12397
HeNBMasterCP_spareAlarmHeNBMasterCP1	12398
HeNBMasterCP_spareAlarmHeNBMasterCP2	12399
HeNBMasterCP_spareAlarmHeNBMasterCP3	12400
HeNBMasterUP_noUserPlaneMapping	12401
HeNB_lteOamConfigurationFailure	12402
HeNB_lteOamConfigurationWarning	12403
HeNB_lteRrcSctpAssociationFailure	12404
LteCell_lteOamCellOperationFailure	12405
LteCell_pciConfusionDetected	12406
VirtualMachineDiskPartition_ vMachineDiskPartitionNearingCapacity	12407
VirtualMachineDisk_vDiskUsageNearingCapacity	12408
VirtualMachineInterface_vLANInterfaceDown	12409
VirtualMachineNIC_vNetworkInterfaceFailure	12410
VirtualMachineNextHopHB_fgwActiveSRLinkDown	12411

VirtualMachineNextHopHB_fgwStandbySRLinkDown	12412
VirtualMachineServer_spareAlarmVirtualMachineServer1	12413
VirtualMachineServer_spareAlarmVirtualMachineServer2	12414
VirtualMachineServer_spareAlarmVirtualMachineServer3	12415
VirtualMachineServer_spareAlarmVirtualMachineServer4	12416
VirtualMachineServer_spareAlarmVirtualMachineServer5	12417
invalidHDMVersion	12418
BackPlaneEPROMFailed	12488
BackPlaneEPROMWarning	12489
healthcheckstatuscluster	12506
oscpuutil	12507

New alarms for 5620 SAM Release 14.0 R7

Alarm name	**Alarm ID**
ScadaBranchSquelched	11240
McLagGatewayPortDown	11241
McLagGatewayPortRedundancyLost	11242
ACCMConfigError	11243
ACCMLoss	11244
CCMContinuityCheckLoss	11245
CollocatedMEPStateDown	11246
ECCMConfigError	11247
ECCMLoss	11248
LocalSignalFailure	11249
MEP1731AIS	11250
MPTermination	11251
OAMMAConfigurationError	11252
OAM_RDI	11253
ODUContinuityCheckLoss	11254
PCCMConfigError	11255
PCCMLoss	11256

PWFail	11257
PWRemotePacketLoss	11258
RDIReceivedInLastACCM	11259
RDIReceivedInLastECCM	11260
RDIReceivedInLastPCCM	11261
RadioLinkStatusDown	11262
RemoteSignalFailure	11263
STM1LPJ2TraceIdentifierMismatch	11264
STM1LpDegrade	11265
STM1LpRemoteDefectIndication	11266
STM1LpRemoteFailureIndication	11267
STM1LpSignalLabelMismatch	11268
STM1LpTuAIS	11269
STM1LpTuLossOfPointer	11270
STM1LpUnequipped	11271
ScheduledActionFailure	11272
ServiceDown	11273
ServicePartial	11274
SynchConfigurationError	11275
SynchMissingSSM	11276
SynchOneSourceDown	11277
SynchQualityLevelDegraded	11278
AesFipsFail	11279
AirLoss	11280
AutonegotiationConfigurationError	11281
AutonegotiationMismatch	11282
CardDisconnected	11283
CardMismatchIndication	11284
E1AISIn	11285
E1AISOut	11286
E1FarEndFailure	11287

E1LoF	11288
E1LoS	11289
E1MaintenanceLoopback	11290
KeyUnavailable	11291
LOF	11292
MauStatusDown	11293
NoPowerSupplyToODU	11294
OpticalSFPLoS	11295
OpticalSFPTXFault	11296
OvercurrentOrUndercurrentFPRPowerSupply	11297
PacketDischarging	11298
PortDown	11299
PortFail	11300
PortSpeedLower	11301
PortSpeedLowerThanCIR	11302
PowerSupplyToODUFailure	11303
PowerSupplyToODUShortCircuit	11304
RadioFrameLoss	11305
RemoteFaultIndication	11306
SFPAbsent	11307
SFPMismatch	11308
SFPRxPowerAbnormal	11309
SFPTxPowerAbnormal	11310
STM1AULossOfPointer	11311
STM1AuAIS	11312
STM1HPDegrade	11313
STM1HPExcessiveError	11314
STM1HPRemoteDefectIndication	11315
STM1HPUnequipped	11316
STM1HighPathSignalLabelMismatch	11317
STM1J0TraceIdentifierMismatch	11318

STM1J1TraceIdentifierMismatch	11319
STM1LoF	11320
STM1LoS	11321
STM1LpTuLossOfMultiframe	11322
STM1MSAIS	11323
STM1MSDegrade	11324
STM1MSExcessiveError	11325
STM1MSFarEndFailure	11326
STM1RSDegrade	11327
CmmLSS_adnsExtendedTTLcaching	11328
CmmLSS_adnsQueryFailureCaching	11329
CmmLSS_adnsQueueCongestion	11330
CmmLSS_cardConnectionLost	11331
CmmLSS_cardStateChange	11332
CmmLSS_cmasFailure	11333
CmmLSS_cmasReceiveFailure	11334
CmmLSS_cmasSendFailure	11335
CmmLSS_cpiAlrmCritical	11336
CmmLSS_cpiAlrmMajor	11337
CmmLSS_cpiAlrmMinor	11338
CmmLSS_cpiAsrtEsc	11339
CmmLSS_cpiAsrtNonEscCritical	11340
CmmLSS_cpiAsrtNonEscMajor	11341
CmmLSS_cpiAsrtNonEscMinor	11342
CmmLSS_cpiAttachFailures	11343
CmmLSS_cpiAttachFailuresSysRelated	11344
CmmLSS_cpiAttachWithPGWreselection	11345
CmmLSS_cpiAttachWithSGWreselection	11346
CmmLSS_cpiCreateDedicatedBearerFailures	11347
CmmLSS_cpiDeactivateDedBearerFailures	11348
CmmLSS_cpiEIRfailuresS13	11349

CmmLSS_cpiExtServiceReqFailuresSysRelated	11350
CmmLSS_cpiExtServiceRequestFailures	11351
CmmLSS_cpiFailuresOverSGs	11352
CmmLSS_cpiFileSysUsage	11353
CmmLSS_cpiGTPcResponseTO_Gn	11354
CmmLSS_cpiGTPcResponseTO_S10	11355
CmmLSS_cpiGTPcResponseTO_S11	11356
CmmLSS_cpiGTPcResponseTO_S3	11357
CmmLSS_cpiGTPcResponseTO_Sv	11358
CmmLSS_cpiHOFailuresTo3G2GOverGn	11359
CmmLSS_cpiHOFailuresToLTEOverGn	11360
CmmLSS_cpiHOfailuresFromGERANoverS3	11361
CmmLSS_cpiHOfailuresFromUTRANoverS3	11362
CmmLSS_cpiHOfailuresRAUto2G3GOverS3	11363
CmmLSS_cpiHOfailuresRAUto2G3GnewSgwOverS3	11364
CmmLSS_cpiHOfailuresRAUto2G3GsameSgwOverS3	11365
CmmLSS_cpiHOfailuresToGERANoverS3	11366
CmmLSS_cpiHOfailurestoUTRANoverS3	11367
CmmLSS_cpiHOwMMErelocFailures_atSource	11368
CmmLSS_cpiHOwMMErelocFailures_atTarget	11369
CmmLSS_cpiHOwNoRelocFailures	11370
CmmLSS_cpiHOwSGWrelocFailures	11371
CmmLSS_cpiHSSauthFailures	11372
CmmLSS_cpiHSSreselection	11373
CmmLSS_cpiMBMSSessionStartM3FailureRate	11374
CmmLSS_cpiMBMSSessionStartSmFailureRate	11375
CmmLSS_cpiMBMSSessionStopM3FailureRate	11376
CmmLSS_cpiMBMSSessionStopSmFailureRate	11377
CmmLSS_cpiMBMSSessionUpdateM3FailureRate	11378
CmmLSS_cpiMBMSSessionUpdateSmFailureRate	11379
CmmLSS_cpiMMEUEcapacity	11380

CmmLSS_cpiMemAllocFail	11381
CmmLSS_cpiMobileTermLocRequestFailures	11382
CmmLSS_cpiNetwrkInducedLocRequestFailures	11383
CmmLSS_cpiNoPSHOFailuresOverSv	11384
CmmLSS_cpiPDNconnWithPGWreselection	11385
CmmLSS_cpiPSHOFailuresOverSv	11386
CmmLSS_cpiReinitServiceSelf	11387
CmmLSS_cpiRestartTask	11388
CmmLSS_cpiS1MMEconnFailures	11389
CmmLSS_cpiS3TauFailures	11390
CmmLSS_cpiS3TauFailuresInterSgw	11391
CmmLSS_cpiS3TauFailuresIntraSGW	11392
CmmLSS_cpiServiceReqFailuresSysRelated	11393
CmmLSS_cpiServiceRequestFailures	11394
CmmLSS_cpiStopWarnMsgDeliveryS1MMEFailureRate	11395
CmmLSS_cpiStopWarnMsgDeliverySBcFailureRate	11396
CmmLSS_cpiTauFailures	11397
CmmLSS_cpiTauFailuresInterMme	11398
CmmLSS_cpiTauFailuresInterMmeInterSgw	11399
CmmLSS_cpiTauFailuresInterSgw	11400
CmmLSS_cpiUEauthFailures	11401
CmmLSS_cpiUpdateBearerFailures	11402
CmmLSS_cpiUpdateDedicatedBearerFailures	11403
CmmLSS_cpiWarnMsgDeliveryS1MMEFailureRate	11404
CmmLSS_cpiWarnMsgDeliverySBcFailureRate	11405
CmmLSS_cpuOverload	11406
CmmLSS_dataMismatch	11407
CmmLSS_degradedResource	11408
CmmLSS_deviceServerCxnLost	11409
CmmLSS_diamLinkDown	11410
CmmLSS_diamMaxClientsExceeded	11411

CmmLSS_dnsThreshold	11412
CmmLSS_ethernetError	11413
CmmLSS_ethernetLinkDown	11414
CmmLSS_excessiveExternalLinksDown	11415
CmmLSS_externalConnectivity	11416
CmmLSS_externalLinkConfigurationLimit	11417
CmmLSS_externalLinkDown	11418
CmmLSS_fqdnError	11419
CmmLSS_ggsnDnsError	11420
CmmLSS_imConnectFailure	11421
CmmLSS_internalCommunicationFailure	11422
CmmLSS_ldapServerConnectionLost	11423
CmmLSS_liNearingCapacityLimit	11424
CmmLSS_linkMOStateChange	11425
CmmLSS_mariadbReplicationDown	11426
CmmLSS_memoryExhaustion	11427
CmmLSS_memoryOverload	11428
CmmLSS_mmeCallTraceStateChange	11429
CmmLSS_mmeDnsError	11430
CmmLSS_mmePcmdStateChange	11431
CmmLSS_mmeTAIeNBMapping	11432
CmmLSS_mmeTAInotSupported	11433
CmmLSS_msThreshold	11434
CmmLSS_msgQueueResource	11435
CmmLSS_noResetAckReceived	11436
CmmLSS_nodeManInhibit	11437
CmmLSS_numberOfTuplesInUse	11438
CmmLSS_pathAvailability	11439
CmmLSS_pgwDnsError	11441
CmmLSS_processDown	11442
CmmLSS_processNotStarted	11443

CmmLSS_progressMarker	11444
CmmLSS_remotedbLinkDown	11445
CmmLSS_sctpEndpointInactive	11446
CmmLSS_serviceCommCxnLost	11447
CmmLSS_sgsnDnsError	11448
CmmLSS_sgwResourceDegraded	11449
CmmLSS_sheddingOverload	11450
CmmLSS_softwareAllocatedResourceOverload	11451
CmmLSS_swVersionMismatch	11452
CmmLSS_taiFqdnError	11453
CmmLSS_tcpDown	11454
CmmLSS_threadsExhausted	11455
CmmLSS_tunnelMonitorHeartbeatFailure	11456
CmmLSS_vLRHostIPconnectionOOS	11457
CmmLSS_vmOverload	11458
CmmUnknownAlarm	11461
adjacencyDown	11462
backhaulServiceDown	11463
inSufficientBandwidth	11464
nonDeployedAdjacencyExists	11465
serviceModified	11466
topologyMisconfigured	11467
RSLHistoryUploadFailure	11468
ATPCAutoDisabled	11469
AccountLogFilledFirstThreshold	11470
AccountLogFilledSecondThreshold	11471
BTSHardwareResynchronization	11472
ConfigurationError	11473
ConfigurationNotSupported	11474
DebugModeOn	11475
FpmrSelfTestFailure	11476

FpmrSystemFailure	11477
FragmentationError	11478
HSBYConfigurationError	11479
HybridPacketMismatch	11480
ManualOperationOn	11481
ModemSignalUnderThreshold	11482
MptSwReconcileFailure	11483
MultipleMatchInPacketIdentification	11484
NEOverheating	11485
NotHybridInterface	11486
ODUSynchMissingSSM	11488
PWFunctionAlarm	11489
ProtectionModeMismatch	11490
RingFailure	11491
RolePriorityMismatch	11492
RxTimerReferenceMissing	11493
SelfTestFailure	11494
SoftwareSwitchNotAllowed	11495
StationAlarmOn	11496
SwHwMismatch	11497
SynchAllSourcesDown	11498
SynchUnlockedPLL	11499
SystemFailure	11500
SystemTypeMismatch	11501
SystemTypeMismatchInPairedODUGroup	11502
TimeServerMissing	11503
TrapOutOfSequence	11504
TxPowerAlarm	11505
USBKeyForWrongNEType	11506
USBKeyNotPresent	11507
USBKeyOverload	11508

USBKeyWithMismatchContent	11509
WrongRoleOrPriorityInPairedODUGroup	11510
PTPClockclassDEG	11511
PTPPeerDelayRespPkt	11512
AUTO_NEGO_MIS_MATCH	11513
BASE_STATION_CONNECTIVITY_DEGRADED	11514
BASE_STATION_CONNECTIVITY_LOST	11515
BASE_STATION_FAULTY	11516
BASE_STATION_LICENSE_LIMITATION	11517
BASE_STATION_NOTIFICATION	11518
BASE_STATION_OPERATION_DEGRADED	11519
BASE_STATION_TRANSMISSION_ALARM	11520
BFD_DOWN	11521
BFD_DOWN_Egress	11522
BFD_DOWN_Ingress	11523
BLUETOOTH_AUTH_FAIL	11524
BLUETOOTH_CONNECTED	11525
BLUETOOTH_ENABLED	11526
BLUETOOTH_PAIRED	11527
CELL_FAULTY	11528
CELL_NOTIFICATION	11529
CELL_OPERATION_DEGRADED	11530
CRL_Update_failure	11531
EXTERNAL_AL_1	11532
EXTERNAL_AL_10	11533
EXTERNAL_AL_11	11534
EXTERNAL_AL_12	11535
EXTERNAL_AL_13	11536
EXTERNAL_AL_14	11537
EXTERNAL_AL_15	11538
EXTERNAL_AL_16	11539

EXTERNAL_AL_17	11540
EXTERNAL_AL_18	11541
EXTERNAL_AL_19	11542
EXTERNAL_AL_2	11543
EXTERNAL_AL_20	11544
EXTERNAL_AL_21	11545
EXTERNAL_AL_22	11546
EXTERNAL_AL_23	11547
EXTERNAL_AL_24	11548
EXTERNAL_AL_25	11549
EXTERNAL_AL_26	11550
EXTERNAL_AL_3	11551
EXTERNAL_AL_4	11552
EXTERNAL_AL_5	11553
EXTERNAL_AL_6	11554
EXTERNAL_AL_7	11555
EXTERNAL_AL_8	11556
EXTERNAL_AL_9	11557
Ethernet_OAM_CCM_fault	11558
Ethernet_OAM_ETH_AIS_fault	11559
FTM_AIS	11560
FTM_BTS_RESET_REQUIRED	11561
FTM_DPD	11562
FTM_EBER	11563
FTM_FAULT_TOGGLING	11564
FTM_LOF	11565
FTM_LOMF	11566
FTM_LOS	11567
FTM_RDI	11568
FTM_RESET	11569
FTM_SECURITY_USER_ACCOUNT	11570

FTM_SFP	11571
FTM_SFP_WARNING	11572
FTM_SYNC_LOSS	11573
FTM_TIMING_SOURCE_LOS	11574
IPSEC_EMERGENCY_BYPASS_ACTIVE	11575
IPSEC_EXPERT_MODE	11576
IPV6_DUPLICATE_ADDRESS_DETECTED	11577
IP_TRAFFIC_CAPTURE_ONGOING	11578
IPsec_tunnel_switchover	11579
LMP_CARRIER_DETECTED	11580
Link_OAM_critical_link_event__alarm	11581
Link_OAM_link_lost_alarm	11582
Link_OAM_loopback_alarm	11583
NEW_CONFIG_REJECTED	11584
NO_CERTIFICATE	11585
NTP_SERVER_UNREACHABLE	11586
PLR_THRESHOLD_CROSSED	11587
RTT_THRESHOLD_CROSSED	11588
SFP_HW_Failure	11589
SSH_ENABLED	11590
SSM_POORQUALITY	11591
SSM_TIMEOUT	11592
TOP_MASTER_UNUSABLE	11593
TRANSPORT_MODULE_MISSING	11594
TRUST_ANCHOR_EXPIRING	11595
UNREGISTERED_ALARM	11596
UNSUPPORTED_HW_DEVICE	11597
VENDOR_CERTIFICATE_EXPIRING	11598
WIFI_CARD_INVALID_TYPE	11599
WIFI_CARD_NOT_PRESENT	11600
ACTIVE_ALARM_OVERFLOW	11601

ALARM_FROM_NE_CORRUPTED	11602
ALARM_LOG_FILE_INACCESSIBLE	11603
ALARM_OVERFLOW_CACHE_FILE_INACCESSIBLE	11604
ALARM_PROCESSOR_CONFIGURATION_IS_OUT_OF_ ORDER	11605
ALARM_SYSTEM_HEARTBEAT	11606
ALARM_SYSTEM_HEARTBEATING_SWITCHED_OFF	11607
ALARM_TYPE_PARAMETER_HAS_BEEN_MODIFIED	11608
APPLICATION_CONFIGURATION_IS_OUT_OF_ORDER	11609
AUTHENTICATION_FAILURE_IN_ETHERNET_DEVICE	11610
BACKEND_DATABASE_REQUIRED_BY_CORBA_ NAMING_SERVICE_IS_UNAVAILABLE	11611
BACKPLANE_LINK_FAULTY	11612
BACKUP_AND_RESTORE_CONNECTION_TO_NETACT_ LOST	11613
BLADECENTER_BLOWER_SPEED_OUT_OF_LIMIT	11614
BLADECENTER_INCOMPATIBLE_HARDWARE_ CONFIGURATION	11615
BLADECENTER_MANAGEMENT_MODULE_ REDUNDANCY_LOST	11616
BLADECENTER_PLUG_IN_UNIT_FAILURE	11617
BLADECENTER_PLUG_IN_UNIT_TEMPERATURE_OUT_ OF_LIMIT	11618
BLADECENTER_PLUG_IN_UNIT_VOLTAGE_OUT_OF_ LIMIT	11619
BLADECENTER_POWER_SUPPLY_FAILURE	11620
BLADECENTER__BLADE_FAILURE	11621
BLADECENTER__CHASSIS_SYSTEM_MANAGEMENT_ FAILURE	11622
BLADECENTER__COOLING_DEVICE_FAILURE	11623
BLADECENTER__I_O_MODULE_FAILURE	11624
BLADECENTER__STORAGE_MODULE_FAILURE	11625
BLADESYSTEM_CHASSIS_POWER_PROBLEM	11626
BLADESYSTEM_FAN_FAILURE	11627

BLADESYSTEM_FUSE_OPEN	11628
BLADESYSTEM_INTERCONNECT_FAILURE	11629
BLADESYSTEM_LINE_VOLTAGE_PROBLEM	11630
BLADESYSTEM_ONBOARD_ADMINISTRATOR_ REDUNDANCY_LOST	11631
BLADESYSTEM_POWER_CHASSIS_NOT_LOAD_ BALANCED	11632
BLADESYSTEM_POWER_ON_FAILED	11633
BLADESYSTEM_POWER_SHED_AUTO_SHUTDOWN	11634
BLADESYSTEM_POWER_SUBSYSTEM_NOT_ REDUNDANT	11635
BLADESYSTEM_POWER_SUBSYSTEM_OVERLOAD_ CONDITION	11636
BLADESYSTEM_POWER_SUPPLY_FAILURE	11637
BLADESYSTEM_REMOTE_INSIGHT_BATTERY_FAILED	11638
BLADESYSTEM_REMOTE_INSIGHT_ERROR	11639
BLADESYSTEM_REMOTE_INSIGHT_POWER_OUTAGE	11640
BLADESYSTEM_TEMPERATURE_OUT_OF_LIMIT	11641
BLADESYSTEM_UNKNOWN_POWER_CONSUMPTION	11642
BLOCK_STORAGE_FOR_ADDITIONAL_PARTITION_ MISSING	11643
BOOTING_FAILURE	11644
BTS_O_M_TOTAL_CONNECTION_LIMIT_EXCEEDED	11645
CANNOT_WRITE_TO_DISK	11646
CAPACITY_USAGE_WARNING_LIMIT_IS_REACHED	11647
CERTIFICATES_DISCREPANCY	11648
CERTIFICATE_CAPACITY_REACHED	11649
CERTIFICATE_EXPIRED	11650
CERTIFICATE_EXPIRING	11651
CERTIFICATE_REVOKED	11652
CLUSTER_OPERATION_INITIATED_BY_OPERATOR	11653
CLUSTER_STARTED__RESTARTED_	11654
CMP_CERT_RETRIEVAL_FAILURE	11655

COMPACTING_IN_MEMORY_DATABASE_FAILED	11656
CONFIGURATION_OF_NWI3_ADAPTER_IS_OUT_OF_ ORDER	11657
CONFIGURATION_OF_SNMP_MEDIATOR_IS_OUT_OF_ ORDER	11658
CONNECTION_LOST_TO_MASTER_FDS_SERVER	11659
CORRUPTED_ALARM_DATA	11660
CORRUPTED_LDAP_DATABASE_RECOVERED	11661
CPU_MALFUNCTION	11662
CPU_USAGE_OVER_LIMIT	11663
CRL_DOWNLOAD_FAILURE	11664
CRL_UPDATE_FAILURE	11665
CURRENT_OUT_OF_LIMIT	11666
DIAMETER_BASE_PROTOCOL_CONFIGURATION_ FAILURE	11667
DISK_DATABASE_IS_GETTING_FULL	11668
DISK_DATABASE_WATCHDOG_START_UP_FAILED	11669
DRBD_HARDWARE_FAILURE	11670
DRBD_SYNCHRONIZATION_FAILURE	11671
ETHERNET_INTERFACE_USAGE_OVER_LIMIT	11672
ETHERNET_LINK_FAILURE	11673
EXCESSIVE_NUMBER_OF_IPMI_EVENTS	11674
EXTERNAL_ETHERNET_SWITCH_CONNECTION_ FAILURE	11675
EXTERNAL_LDAP_FAILURE	11676
EXTERNAL_STORAGE_SYSTEM_FAILURE	11677
EXTERNAL_USER_ACCOUNT_VALIDATION_FAILED	11678
FAILED_TO_CREATE_NETACT_CONNECTION	11679
FALLBACK_OCCURED	11680
FAST_DATA_STRUCTURE_AUTOMATIC_RECOVERY_ FAILED	11681
FAST_DATA_STRUCTURE_IS_CORRUPTED	11682
FAST_DATA_STRUCTURE_START_UP_FAILED	11683

FIBRE_CHANNEL_CONTROLLER_ERROR	11684
FIBRE_CHANNEL_DEVICE_ERROR	11685
FIBRE_CHANNEL_FRAME_TRANSMISSION__CRC__ ERROR	11686
FIBRE_CHANNEL_LINK_ERROR	11687
FIBRE_CHANNEL_LINK_FAILURE	11688
FIBRE_CHANNEL_SWITCH_PORT_STATUS_CHANGE	11689
FIBRE_CHANNEL_SWITCH_STATUS_CHANGE	11690
FIBRE_CHANNEL_TOTAL_LOSS_OF_SYNC	11691
FIELD_REPLACEABLE_UNIT_UNAVAILABLE	11692
FILE_SYSTEM_USAGE_OVER_LIMIT	11693
FRONTPANEL_LINK_FAULTY	11694
FailedStatsCollectionAtAcknowledge	11695
FailedStatsProcessing	11696
GUEST_HW_MISCONFIGURATION	11697
HARD_DISK_DRIVE_FAILURE	11698
ID_CONFLICT_IN_BTS_O_M_CONNECTION	11699
ILLEGAL_USAGE_OF_EXTERNAL_ALARM_TIME	11700
INCOMPLETE_OR_CORRUPTED_USER_DATA_FOR_ VIRTUAL_OMS_DEPLOYMENT	11701
INCORRECT_ALARM_DATA	11702
INCORRECT_BIOS_SETTINGS	11703
INCORRECT_CONFIGURATION_DATA_IN_LDAP	11704
INSECURE_O_M_CONNECTION	11705
INVALID_ACTIVE_SESSIONS	11706
INVALID_IP_CONFIGURATION	11707
INVALID_SNMP_TRAP_COMMUNITY_STRING	11708
IN_MEMORY_DATABASE_DISK_PARTITION_PROBLEM_ DETECTED	11709
IN_MEMORY_DATABASE_IS_ERRONEOUSLY_ CONFIGURED	11710
IN_MEMORY_DATABASE_IS_FAULTY	11711

IN_MEMORY_DATABASE_PARTITION_GETTING_FULL	11712
IN_MEMORY_DATABASE_SERVER_IS_FAULTY	11713
IN_MEMORY_DATABASE_SWITCHED_TO_LESS_ RELIABLE_REPLICATION_PROTOCO	11714
IN_MEMORY_DATABASE_WATCHDOG_START_UP_ FAILED	11715
IPMI_INTERNAL_FAILURE	11716
JUNIPER_NEW_MASTER_IN_VIRTUAL_ROUTER_ REDUNDANCY_PROTOCOL_MODE	11717
JUNIPER_SWITCH_FAN_FAILURE	11718
JUNIPER_SWITCH_FIELD_REPLACEABLE_UNIT_ FAILURE_	11719
JUNIPER_SWITCH_OVER_TEMPERATURE	11720
JUNIPER_SWITCH_POWER_SUPPLY_FAILURE_	11721
LDAP_DATABASE_CORRUPTED	11722
LICENCE_DATA_IS_CORRUPTED	11723
LICENSE_MANAGEMENT_INTERNAL_MESSAGE_ AUTHENTICATION_FAILED	11724
MAJOR_SW_UPGRADE_DATA_IMPORT_FAILURE	11725
MANAGED_OBJECT_FAILED	11726
MANAGED_OBJECT_LOCKED	11727
MANAGED_OBJECT_SHUTDOWN_BY_OPERATOR	11728
MANAGED_OBJECT_UNLOCKED_BY_OPERATOR	11729
MANUAL_NODE_ISOLATION_VERIFICATION_NEEDED	11730
MAXIMUM_THRESHOLD_HAS_BEEN_CROSSED	11731
MEASUREMENT_DATA_ERROR	11732
MEASUREMENT_DATA_NOT_TRANSFERRED	11733
MEASUREMENT_THRESHOLD_MONITORING_LIMIT_ EXCEEDED	11734
MEMORY_ERROR	11735
MEMORY_USAGE_OVER_LIMIT	11736
MINIMUM_THRESHOLD_HAS_BEEN_REACHED	11737
MissedStatsCollectionAtRecovery	11738

MissedStatsCollectionAtRequest	11739
NE_CONNECTION_REJECTED	11740
NE_O_M_CONNECTION_FAILURE	11741
NE_O_M_UPDATE_CRL_MEDIATION_FAILURE	11742
NODE_FAILED	11743
NODE_NOT_RESPONDING	11744
NO_OPERATIONAL_RECOVERY_UNIT_FOR_SERVICE_INSTANCE	11745
NO_REPLY_TO_SNMP_REQUEST	11746
NTP_TIME_SYNCHRONISATION_LEADING_TO_LDAP_REPLICATION_FAILURE	11747
NUMBER_OF_SYNHCRONOUS_REPLICAS_TOO_LOW	11748
NWI3_NOTIFICATION_MISSING	11749
OMS_ALARM_UPLOAD_FROM_NE_FAILED	11750
OMS_FILE_TRANSFER_CONNECTION_COULD_NOT_BE_OPENED	11751
OMS_MEASUREMENT_DATA_PROCESSING_OVERLOAD	11752
OPERATING_SYSTEM_MONITORING_FAILURE	11753
ORACLE_CLUSTER_ALERT	11754
ORACLE_CLUSTER_ASM_GROUP_IS_GETTING_FULL	11755
ORACLE_CLUSTER_COMPONENT_IS_FAULTY	11756
O_M_MEDIATION_FAILURE	11757
PLUG_IN_UNIT_FAILURE	11758
PLUG_IN_UNIT_TEMPERATURE_OUT_OF_LIMIT	11759
PLUG_IN_UNIT_VOLTAGE_OUT_OF_LIMIT	11760
PM_FTP_CONNECTION_FAILED	11761
POSSIBLE_SECURITY_THREAT_IN_NETWORK_ELEMENT	11762
POWER_SUPPLY_FAILURE	11763
PROCESSING_OF_ALARMS_IS_STARTED_ANEW	11764
PROCESS_START_UP_FAILED_DUE_TO_AN_UNAVAILABLE_SERVICE	11765
RAID_ARRAY_HAS_BEEN_DEGRADED	11766

RECOVERY_ACTIONS_BANNED_FOR_MANAGED_ OBJECT	11767
RECOVERY_GROUP_SWITCHOVER	11768
RECREATING_STANDBY_IN_MEMORY_DATABASE_ FAILED	11769
REPLICATION_FAILING_FOR_IN_MEMORY_DATABASE	11770
RESOURCE_ALLOCATION_OR_DE_ALLOCATION_ FAILURE	11771
RUIMRMEX_LDAP_DATA_DISTRIBUTION_FAILURE	11772
RegistrationServiceConfiguration	11773
SERVICE_LEVEL_DEGRADED_BELOW_THRESHOLD	11774
SS7___SIGTRAN_PROTOCOL_STACK_ CONFIGURATION_FAILURE	11775
SSL_CONNECTION_CANNOT_BE_MADE_BY_RUIM	11776
STAGING_AREA_IN_INCONSISTENT_STATE	11777
SWITCH_AND_SERVICE_UNIT__FABRIC_BROADCAST_ STORM	11778
SWITCH_AND_SERVICE_UNIT__IPMI_SYSTEM_EVENT_ LOG_FULL	11779
SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_ MEMORY_FULL	11780
SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_ RESTART	11781
SWITCH_AND_SERVICE_UNIT__RSTP_NEW_ROOT	11782
SWITCH_AND_SERVICE_UNIT___RSTP__TOPOLOGY_ CHANGE	11783
SWITCH_FAULTY	11784
SWITCH_LINK_DOWN	11785
SWITCH_RESTARTED	11786
SW_SET_ACTIVATION_FAILED	11787
SW_SET_POSTACTIVATION_SCRIPT_EXECUTION_ ERROR	11788
SYSTEM_CLOCK_OUT_OF_SYNC_WITH_NTP_SERVER	11789
TAKING_CHECKPOINT_OF_IN_MEMORY_DATABASE_ FAILED	11790

TAKING_SCHEDULED_CHECKPOINT_OF_IN_MEMORY_ DATABASE_FAILED	11791
THRESHOLD_MONITORING_LIMIT_EXCEEDED	11792
THRESHOLD_VALUE_EXCEEDED_IN_ETHERNET_ DEVICE	11793
TRACE_CONNECTION_TO_NE_IS_LOST	11794
TROUBLESHOOTING_DATA_CREATION_OR_UPLOAD_ FAILED	11795
TROUBLESHOOTING_DATA_RECEIVED	11796
UNEXPECTED_CONNECTIONS_TO_IN_MEMORY_ DATABASE_HAVING_STANDBY_ROLE	11797
UNEXPECTED_PERSISTENT_STATUS_DATA_VALUES_ FOR_IN_MEMORY_DATABASE	11798
UNKNOWN_SNMP_TRAP	11799
UNKNOWN_SPECIFIC_PROBLEM	11800
UNRECOMMENDED_CONFIGURATION_FORCED_BY_ OPERATOR	11801
VOLTAGE_OUT_OF_LIMIT	11802
WARNINGS_REPORTED_FOR_MSU_AUTOMATIC_ POSTCONFIGURATION	11803
WCEL_THRESHOLD_MONITORING_LIMIT_EXCEEDED	11804
WEBSPHERE_INTERNAL_ERROR	11805
BTSSoftwareResynchronization	11806
BTSSoftwareUpgrade	11807
OAMDiscoveryFail	11808
ODUODUPortFailure	11809
CmmCinderVolumeContentUnexpected	11810
CmmCinderVolumeRemoved	11811
CmmLSS_ethernetLinkStateChange	11812
CmmLSS_excessiveExtCommFailure	11813
CmmLSS_externalCommFailure	11814
CmmLSS_fcClientAppConfigErr	11815
CmmLSS_hostReset	11816

CmmLSS_mmeConnectionLost	11817
CmmLSS_mmeControllerOOS	11818
CmmLSS_provisioningError	11819
CmmLSS_sctpPriPathInconsistency	11820
CmmLowMemoryResourceDbs	11821
CmmSystemServiceUnavailable	11822
CmmVmUnreachable	11823

New alarms for 5620 SAM Release 14.0 R5

Alarm name	**Alarm ID**
AaTcpValTcaCrossed	11057
PccRuleInsertSpaceThresholdAlarm	11058
PccRuleInsertedFltrEntryDropped	11059
NsgVirtualSwitchDown	11060
NsgVirtualSwitchPartiallyDown	11061
UplinkDown	11062
UplinkPartiallyDown	11063
DhcpServerAddrAllocationFailure	11064
DhcpServerHostConflict	11065
DhcpServerIntLseConflict	11066
DhcpServerLeaseNotOwner	11067
DhcpServerLeaseOfferedExpired	11068
DhcpServerPoolUnknown	11069
PacketDropped	11070
AmpDisabledC	11071
AmpDisabledL	11072
AmpGainTooHighC	11073
AmpGainTooHighL	11074
AmpGainTooLowC	11075
AmpGainTooLowL	11076
BdLnkSpd	11077

CBandLossOfSignalC	11078
CBandLossOfSignalL	11079
CKWKATMismatch	11080
CardFailCru	11081
CardPowerOff	11082
CardThermShutdown	11083
EcModeMismatch	11084
EcTypeMismatch	11085
FaceplateMissing	11086
FirmwareErrorAlarm	11087
HwrvUnknown	11088
IPSecIsaMemoryHigh	11089
IPSecIsaMemoryMax	11090
IntOhFail	11091
IntTsiFailure	11092
InvalidModule	11093
InvalidXc	11094
InventoryErrMod	11095
LnkSpdDeg	11096
LossOfSignalC	11097
LossOfSignalL	11098
LotOutC	11099
LotOutL	11100
MepFacilityFault	11101
OAPumpLaserBiasCurrentHighC	11102
OAPumpLaserBiasCurrentHighL	11103
OAPumpLaserTempHighC	11104
OAPumpLaserTempHighL	11105
OesFanSpeedHigh	11106
OesFanSpeedLow	11107
OesFirmwareCondition	11108

OesNtpOutOfSync	11109
OesOpticalTrnspndrMiscFailAlarm	11110
OesRedundancyFail	11111
OprPwrHighC	11112
OprPwrHighL	11113
OprPwrLowC	11114
OprPwrLowL	11115
PwrMaxGainC	11116
PwrMaxGainL	11117
SC1LinkDegrade	11118
SC1LinkFail	11119
SC2LinkDegrade	11120
SC2LinkFail	11121
SC3LinkDegrade	11122
SC3LinkFail	11123
SCLinkDegrade	11124
SCLinkFail	11125
ShelfAirFilterMaintenance	11126
ShelfInventoryError	11127
ShelfInventoryMismatch	11128
SoftwareError	11129
SyncChannelA	11130
SyncChannelB	11131
SyncChannelBoth	11132
XcMismatch	11133
osuCardUnknown	11134
osuInMaintenance	11135
osuIntTempHigh	11136
osuSoftwareUpgradeFailure	11137
osuSoftwareVersionMismatch	11138
AVCNOverload	11139

BSR_missedTriggeringSelfOpt	11140
BSR_mnoDataUpdateFailure	11141
BSR_msAPoutOfMemory	11142
BSR_scepInvalidConfiguration	11143
BSR_scepProtocolError	11144
BSR_scepProvisionedCertMismatch	11145
FGW_logFileTransferFailure	11146
FGW_secHardeningProcedureFailure	11147
HDMConfiguration_ FileserverHostNameForFemtoConfigurationAlarm	11148
HDMConfiguration_OamNeIPConfigurationAlarm	11149
HeNB_errorContactingBaImCalibrationServer	11150
HeNB_errorContactingBaImThroughputSamplingServer	11151
HeNB_errorCrmUnableToProvideLteuService	11152
HeNB_spareHeNBAlarm4	11153
HeNB_spareHeNBAlarm5	11154
HeNB_spareHeNBAlarm6	11155
LCell_sleepingCellDetected	11156
LteCell_collidingPciSelected	11157
LteCell_lteSleepingCellDetected	11158
LteCell_ueAuditContextMismatch	11159
LteCell_ueAuditGbrUsageMismatch	11160
OAM_222	11161
OAM_225	11162
SCTPAssociation_remoteSCTPCommDown	11163
SCTPAssociation_sCTPPeerRestart	11164
alarmOverload	11165
applicationalarmOverload	11166
bulkoperationresultOverload	11167
deviceactionresultOverload	11168
devicedeletionnotificationOverload	11169

deviceinformeventOverload	11170
deviceregistrationOverload	11171
operationresultOverload	11172
resyncEventsOverload	11173
IsaDatapathCpuUsage	11174
DuplicateNodeIPv6SegmentId	11175
liMirrorLiNat64SubOperStateDown	11176
AlarmDebouncingThresholdReached	11177
DbCrcTypeMis	11178
NoSFMConfigured	11179
oesCfgBlocked	11180
oesCfgFailNoMemory	11181
oesSwBelowMinRev	11182
oesSwUpgdCleanupFailed	11183
oesSwUpgdFailed	11184
PXCAdministrativelyDown	11185
PXCDown	11186
RipInterfaceDown	11187
CpmProtectionViolationVdoSvcEntry	11188
CpmProtectionViolationVdoVrtrClientEntry	11189
KPIThresholdCrossingAlarm	11190
SerialControlLeadsSignalChange	11191
CabinAlarm1	11192
CabinAlarm2	11193
CabinAlarm3	11194
CabinAlarm4	11195
FrameAlarm1	11196
FrameAlarm10	11197
FrameAlarm11	11198
FrameAlarm12	11199
FrameAlarm2	11200

FrameAlarm3	11201
FrameAlarm4	11202
FrameAlarm5	11203
FrameAlarm6	11204
FrameAlarm7	11205
FrameAlarm8	11206
FrameAlarm9	11207
UserAlarm1	11208
UserAlarm10	11209
UserAlarm11	11210
UserAlarm12	11211
UserAlarm13	11212
UserAlarm14	11213
UserAlarm15	11214
UserAlarm16	11215
UserAlarm17	11216
UserAlarm18	11217
UserAlarm19	11218
UserAlarm2	11219
UserAlarm20	11220
UserAlarm21	11221
UserAlarm22	11222
UserAlarm23	11223
UserAlarm24	11224
UserAlarm25	11225
UserAlarm26	11226
UserAlarm27	11227
UserAlarm28	11228
UserAlarm29	11229
UserAlarm3	11230
UserAlarm30	11231

UserAlarm31	11232
UserAlarm32	11233
UserAlarm4	11234
UserAlarm5	11235
UserAlarm6	11236
UserAlarm7	11237
UserAlarm8	11238
UserAlarm9	11239

New alarms for 5620 SAM Release 14.0 R3

Alarm name	**Alarm ID**
BareMetalReachabilityDown	10273
HostPortReachabilityDown	10274
LagPortDown	10275
RxProblem	10276
TrafficDown	10277
TrafficLoss	10278
TxProblem	10279
FastPhotonicRestModeMismatch	10280
IK8000160	10281
IK8000161	10282
IK8000162	10283
IK8000163	10284
IK8000164	10285
IK8000165	10286
IK8000166	10287
IK8000167	10288
IK8000169	10289
IK8000170	10290
IK8000171	10291
IK8000172	10292

IK8000174	10293
IK8000175	10294
IK8000176	10295
IK8000203	10296
IK8000562	10297
IK8000563	10298
IK8000564	10299
IK8000565	10300
IK8000614	10301
IK8000615	10302
IK8000616	10303
IK8000617	10304
IK8000618	10305
IK8000619	10306
IK8000620	10307
IK8000621	10308
IK8000622	10309
IK8000623	10310
IK8000624	10311
IK8000625	10312
IK8010107	10313
IK8010552	10314
IK8010562	10315
IK8010611	10316
IK8010641	10317
IK8010651	10318
IK8020201	10319
IK8020230	10320
IK8100081	10321
IK8100104	10322
IK8100105	10323

IK8361018	10324
IK8361033	10325
IK8361040	10326
IK8361091	10327
IK8361102	10328
IK8361105	10329
IK8361125	10330
IK8361135	10331
IK8361154	10332
IK8361160	10333
IK8361163	10334
IK8362337	10335
IK8362341	10336
IK8362343	10337
IK8362349	10338
IK8362360	10339
IK8362401	10340
IK8362409	10341
IK8362462	10342
IK8362464	10343
IK8362468	10344
IK8362494	10345
IK8362496	10346
IK8362508	10347
IK8362510	10348
IK8362518	10349
IK8362531	10350
IK8362533	10351
IK8362534	10352
IK8362536	10353
IK8362539	10354

IK8362541	10355
IK8362543	10356
IK8362546	10357
IK8362548	10358
IK8362550	10359
IK8362552	10360
IK8362554	10361
IK8362556	10362
IK8362559	10363
IK8362609	10364
IK8362633	10365
IK8362636	10366
IK8362648	10367
IK8362657	10368
IK8362748	10369
IK8367481	10370
IK8367482	10371
IK8367483	10372
IK8367484	10373
IK8367485	10374
IK8367486	10375
IK8367487	10376
IK8367488	10377
IK8367489	10378
IK8367490	10379
IK8367491	10380
IK8367500	10381
IK8367501	10382
IK8367502	10383
IK8367503	10384
IK8367504	10385

IK8367505	10386
IK8367508	10387
IK8367509	10388
IK8367510	10389
IK8367511	10390
IK8367512	10391
IK8367513	10392
IK8367514	10393
IK8367515	10394
IK8367516	10395
IK8367517	10396
IK8367518	10397
IK8367519	10398
IK8367520	10399
IK8367521	10400
IK8367522	10401
IK8367523	10402
IK8367524	10403
IK8367525	10404
IK8367526	10405
IK8367527	10406
IK8367528	10407
IK8367529	10408
IK8367530	10409
IK8367531	10410
IK8367532	10411
IK8367533	10412
IK8367534	10413
IK8367535	10414
IK8367536	10415
IK8367537	10416

IK8367538	10417
IK8367539	10418
IK8367540	10419
IK8367541	10420
IK8367542	10421
IK8367543	10422
IK8367545	10423
IK8367546	10424
IK8367547	10425
IK8367548	10426
IK8367549	10427
IK8367550	10428
IK8367551	10429
IK8367552	10430
IK8367553	10431
IK8367554	10432
IK8367555	10433
IK8367556	10434
IK8367557	10435
IK8367558	10436
IK8367559	10437
IK8367560	10438
IK8367561	10439
IK8367562	10440
IK8367563	10441
IK8367564	10442
IK8367565	10443
IK8367566	10444
IK8367567	10445
IK8367568	10446
IK8367569	10447

IK8367570	10448
IK8367571	10449
IK8367572	10450
IK8367573	10451
IK8367574	10452
IK8367575	10453
IK8367576	10454
IK8367577	10455
IK8367578	10456
IK8367579	10457
IK8367580	10458
IK8367581	10459
IK8367582	10460
IK8367583	10461
IK8367584	10462
IK8367585	10463
IK8367586	10464
IK8367587	10465
IK8367588	10466
IK8367589	10467
IK8367590	10468
IK8367591	10469
IK8367592	10470
IK8367593	10471
IK8367594	10472
IK8367595	10473
IK8367596	10474
IK8367597	10475
IK8367598	10476
IK8367599	10477
IK8367600	10478

IK8367601	10479
IK8367602	10480
IK8367603	10481
IK8367604	10482
IK8367605	10483
IK8367606	10484
IK8367607	10485
IK8457481	10486
IK8457482	10487
IK8457483	10488
IK8457484	10489
IK8457485	10490
IK8457486	10491
IK8457487	10492
IK8457488	10493
IK8457489	10494
IK8457490	10495
IK8457491	10496
IK8457492	10497
IK8457493	10498
IK8457494	10499
IK8457495	10500
IK8457496	10501
IK8457497	10502
IK8457498	10503
IK8457500	10504
IK8457501	10505
IK8457502	10506
IK8457503	10507
IK8457504	10508
IK8457505	10509

IK8457506	10510
IK8457507	10511
IK8457508	10512
IK8457509	10513
IK8457510	10514
IK8457511	10515
IK8457512	10516
IK8457513	10517
IK8457514	10518
IK8457515	10519
IK8457516	10520
IK8457517	10521
IK8457518	10522
IK8457519	10523
IK8457520	10524
IK8457521	10525
IK8457522	10526
IK8457523	10527
IK8457524	10528
IK8457525	10529
IK8457526	10530
IK8457527	10531
IK8457528	10532
IK8457529	10533
IK8457530	10534
IK8457531	10535
IK8457532	10536
IK8457533	10537
IK8457534	10538
IK8457535	10539
IK8457536	10540

IK8457537	10541
IK8457538	10542
IK8457539	10543
IK8457540	10544
IK8457541	10545
IK8457542	10546
IK8457543	10547
IK8457544	10548
IK8457545	10549
IK8457546	10550
IK8457547	10551
IK8457548	10552
IK8457549	10553
IK8457550	10554
IK8457551	10555
IK8457552	10556
IK8457553	10557
IK8457554	10558
IK8457555	10559
IK8457556	10560
IK8457557	10561
IK8457558	10562
IK8457559	10563
IK8457560	10564
IK8457561	10565
IK8457562	10566
IK8457563	10567
IK8457564	10568
IK8457565	10569
IK8457566	10570
IK8457567	10571

IK8457568	10572
IK8457569	10573
IK8457570	10574
IK8457571	10575
IK8457572	10576
IK8457573	10577
IK8457574	10578
IK8457575	10579
IK8457576	10580
IK8457577	10581
IK8457578	10582
IK8457579	10583
IK8457580	10584
IK8457581	10585
IK8457582	10586
IK8457583	10587
IK8457584	10588
IK8457585	10589
IK8457586	10590
IK8457587	10591
IK8457588	10592
IK8457589	10593
IK8457590	10594
IK8457591	10595
IK8457592	10596
IK8457593	10597
IK8457594	10598
IK8457595	10599
IK8457596	10600
IK8457597	10601
IK8457598	10602

IK8457599	10603
IK8457600	10604
IK8457601	10605
IK8457602	10606
IK8457603	10607
IK8457604	10608
IK8457605	10609
IK8457606	10610
IK8457607	10611
IK8557481	10612
IK8557482	10613
IK8557483	10614
IK8557484	10615
IK8557485	10616
IK8557486	10617
IK8557487	10618
IK8557488	10619
IK8557489	10620
IK8557490	10621
IK8557491	10622
IK8557500	10623
IK8557501	10624
IK8557502	10625
IK8557503	10626
IK8557504	10627
IK8557505	10628
IK8557508	10629
IK8557509	10630
IK8557510	10631
IK8557511	10632
IK8557512	10633

IK8557513	10634
IK8557514	10635
IK8557515	10636
IK8557516	10637
IK8557517	10638
IK8557518	10639
IK8557519	10640
IK8557520	10641
IK8557521	10642
IK8557522	10643
IK8557523	10644
IK8557524	10645
IK8557525	10646
IK8557526	10647
IK8557527	10648
IK8557528	10649
IK8557529	10650
IK8557530	10651
IK8557531	10652
IK8557532	10653
IK8557533	10654
IK8557534	10655
IK8557535	10656
IK8557536	10657
IK8557537	10658
IK8557538	10659
IK8557539	10660
IK8557540	10661
IK8557541	10662
IK8557542	10663
IK8557543	10664

IK8557545	10665
IK8557546	10666
IK8557547	10667
IK8557548	10668
IK8557549	10669
IK8557550	10670
IK8557551	10671
IK8557552	10672
IK8557553	10673
IK8557554	10674
IK8557555	10675
IK8557556	10676
IK8557557	10677
IK8557558	10678
IK8557559	10679
IK8557560	10680
IK8557561	10681
IK8557562	10682
IK8557563	10683
IK8557564	10684
IK8557565	10685
IK8557566	10686
IK8557567	10687
IK8557568	10688
IK8557569	10689
IK8557570	10690
IK8557571	10691
IK8557572	10692
IK8557573	10693
IK8557574	10694
IK8557575	10695

IK8557576	10696
IK8557577	10697
IK8557578	10698
IK8557579	10699
IK8557580	10700
IK8557581	10701
IK8557582	10702
IK8557583	10703
IK8557584	10704
IK8557585	10705
IK8557586	10706
IK8557587	10707
IK8557588	10708
IK8557589	10709
IK8557590	10710
IK8557591	10711
IK8557592	10712
IK8557593	10713
IK8557594	10714
IK8557595	10715
IK8557596	10716
IK8557597	10717
IK8557598	10718
IK8557599	10719
IK8557600	10720
IK8557601	10721
IK8557602	10722
IK8557603	10723
IK8557604	10724
IK8557605	10725
IK8557606	10726

IK8557607	10727
IK8600385	10728
IK8609980	10729
IK8609981	10730
IK8609982	10731
IK8609983	10732
IK8609984	10733
IK8609985	10734
IK8609986	10735
IK8609987	10736
IK8609988	10737
IK8609989	10738
IK8609990	10739
IK8609991	10740
IK8609992	10741
IK8609993	10742
IK8609994	10743
IK8609995	10744
IK8609996	10745
IK8609997	10746
IK8609998	10747
IK8609999	10748
IK8610350	10749
IK8619980	10750
IK8619981	10751
IK8619982	10752
IK8619983	10753
IK8619984	10754
IK8619985	10755
IK8619986	10756
IK8619987	10757

IK8619988	10758
IK8619989	10759
IK8619990	10760
IK8619991	10761
IK8619992	10762
IK8619993	10763
IK8619994	10764
IK8619995	10765
IK8619996	10766
IK8619997	10767
IK8619998	10768
IK8619999	10769
IK8657481	10770
IK8657482	10771
IK8657483	10772
IK8657484	10773
IK8657485	10774
IK8657486	10775
IK8657487	10776
IK8657488	10777
IK8657489	10778
IK8657490	10779
IK8657491	10780
IK8657500	10781
IK8657501	10782
IK8657502	10783
IK8657503	10784
IK8657504	10785
IK8657505	10786
IK8657508	10787
IK8657509	10788

IK8657510	10789
IK8657511	10790
IK8657512	10791
IK8657513	10792
IK8657514	10793
IK8657515	10794
IK8657516	10795
IK8657517	10796
IK8657518	10797
IK8657519	10798
IK8657520	10799
IK8657521	10800
IK8657522	10801
IK8657523	10802
IK8657524	10803
IK8657525	10804
IK8657526	10805
IK8657527	10806
IK8657528	10807
IK8657529	10808
IK8657530	10809
IK8657531	10810
IK8657532	10811
IK8657533	10812
IK8657534	10813
IK8657535	10814
IK8657536	10815
IK8657537	10816
IK8657538	10817
IK8657539	10818
IK8657540	10819

IK8657541	10820
IK8657542	10821
IK8657543	10822
IK8657545	10823
IK8657546	10824
IK8657547	10825
IK8657548	10826
IK8657549	10827
IK8657550	10828
IK8657551	10829
IK8657552	10830
IK8657553	10831
IK8657554	10832
IK8657555	10833
IK8657556	10834
IK8657557	10835
IK8657558	10836
IK8657559	10837
IK8657560	10838
IK8657561	10839
IK8657562	10840
IK8657563	10841
IK8657564	10842
IK8657565	10843
IK8657566	10844
IK8657567	10845
IK8657568	10846
IK8657569	10847
IK8657570	10848
IK8657571	10849
IK8657572	10850

IK8657573	10851
IK8657574	10852
IK8657575	10853
IK8657576	10854
IK8657577	10855
IK8657578	10856
IK8657579	10857
IK8657580	10858
IK8657581	10859
IK8657582	10860
IK8657583	10861
IK8657584	10862
IK8657585	10863
IK8657586	10864
IK8657587	10865
IK8657588	10866
IK8657589	10867
IK8657590	10868
IK8657591	10869
IK8657592	10870
IK8657593	10871
IK8657594	10872
IK8657595	10873
IK8657596	10874
IK8657597	10875
IK8657598	10876
IK8657599	10877
IK8657600	10878
IK8657601	10879
IK8657602	10880
IK8657603	10881

IK8657604	10882
IK8657605	10883
IK8657606	10884
IK8657607	10885
IK8757481	10886
IK8757482	10887
IK8757483	10888
IK8757484	10889
IK8757485	10890
IK8757486	10891
IK8757487	10892
IK8757488	10893
IK8757489	10894
IK8757490	10895
IK8757491	10896
IK8757500	10897
IK8757501	10898
IK8757502	10899
IK8757503	10900
IK8757504	10901
IK8757505	10902
IK8757508	10903
IK8757509	10904
IK8757510	10905
IK8757511	10906
IK8757512	10907
IK8757513	10908
IK8757514	10909
IK8757515	10910
IK8757516	10911
IK8757517	10912

IK8757518	10913
IK8757519	10914
IK8757520	10915
IK8757521	10916
IK8757522	10917
IK8757523	10918
IK8757524	10919
IK8757525	10920
IK8757526	10921
IK8757527	10922
IK8757528	10923
IK8757529	10924
IK8757530	10925
IK8757531	10926
IK8757532	10927
IK8757533	10928
IK8757534	10929
IK8757535	10930
IK8757536	10931
IK8757537	10932
IK8757538	10933
IK8757539	10934
IK8757540	10935
IK8757541	10936
IK8757542	10937
IK8757543	10938
IK8757545	10939
IK8757546	10940
IK8757547	10941
IK8757548	10942
IK8757549	10943

IK8757550	10944
IK8757551	10945
IK8757552	10946
IK8757553	10947
IK8757554	10948
IK8757555	10949
IK8757556	10950
IK8757557	10951
IK8757558	10952
IK8757559	10953
IK8757560	10954
IK8757561	10955
IK8757562	10956
IK8757563	10957
IK8757564	10958
IK8757565	10959
IK8757566	10960
IK8757567	10961
IK8757568	10962
IK8757569	10963
IK8757570	10964
IK8757571	10965
IK8757572	10966
IK8757573	10967
IK8757574	10968
IK8757575	10969
IK8757576	10970
IK8757577	10971
IK8757578	10972
IK8757579	10973
IK8757580	10974

IK8757581	10975
IK8757582	10976
IK8757583	10977
IK8757584	10978
IK8757585	10979
IK8757586	10980
IK8757587	10981
IK8757588	10982
IK8757589	10983
IK8757590	10984
IK8757591	10985
IK8757592	10986
IK8757593	10987
IK8757594	10988
IK8757595	10989
IK8757596	10990
IK8757597	10991
IK8757598	10992
IK8757599	10993
IK8757600	10994
IK8757601	10995
IK8757602	10996
IK8757603	10997
IK8757604	10998
IK8757605	10999
IK8757606	11000
IK8757607	11001
GwMscpUeIdUsgAlarm	11002
IK4004263	11003
IK4004264	11004
IK4004265	11005

IK4004267	11006
IK4004272	11007
IK4007318	11008
IK4007319	11009
IK4007320	11010
IK4007321	11011
IK4007322	11012
IK4007323	11013
IK4007324	11014
IK4007325	11015
IK4009321	11016
IK4009324	11017
IK4009325	11018
IK4009326	11019
IK4009327	11020
IK4010053	11021
IK4012095	11022
IK4012096	11023
IK4012097	11024
IK4012098	11025
IK4201033	11026
IK4305257	11027
IK4305258	11028
IK4305259	11029
IK4305260	11030
IK4305261	11031
IK4306412	11032
IK4306413	11033
IK4306414	11034
IK4306416	11035
IK4306418	11036

IK4306419	11037
IK4306420	11038
IK4306421	11039
IK4306422	11040
IK4306423	11041
IK4306424	11042
IK4306425	11043
IK4306426	11044
IK4306427	11045
IK4306428	11046
IK4306429	11047
IK4306430	11048
IK4306431	11049
IK4306432	11050
IK4500164	11051
IK4500165	11052
IK4500166	11053
IK4500167	11054
IK4500168	11055
BofSaveFailed	11056

New alarms for 5620 SAM Release 14.0 R1

Alarm name	Alarm ID
IK8752443	10000
IK8752444	10001
IK8752462	10002
IK8752464	10003
IK8752468	10004
IK8752490	10005
IK8752493	10006
IK8752494	10007

IK8752496	10008
IK8752499	10009
IK8752500	10010
IK8752502	10011
IK8752503	10012
IK8752504	10013
IK8752507	10014
IK8752508	10015
IK8752510	10016
IK8752512	10017
IK8752513	10018
IK8752518	10019
IK8752526	10020
IK8752527	10021
IK8752528	10022
IK8752529	10023
IK8752531	10024
IK8752533	10025
IK8752534	10026
IK8752536	10027
IK8752538	10028
IK8752539	10029
IK8752541	10030
IK8752543	10031
IK8752545	10032
IK8752546	10033
IK8752548	10034
IK8752550	10035
IK8752552	10036
IK8752554	10037
IK8752556	10038

IK8850006	10039
CmuManagementFailed	10040
IK4001044	10041
IK4001045	10042
IK4002023	10043
IK4002024	10044
IK4002025	10045
IK4003149	10046
IK4003153	10047
IK4003154	10048
IK4004257	10049
IK4004258	10050
IK4004259	10051
IK4004260	10052
IK4005101	10053
IK4005102	10054
IK4006354	10055
IK4006355	10056
IK4007280	10057
IK4007281	10058
IK4007282	10059
IK4007283	10060
IK4007284	10061
IK4007285	10062
IK4007286	10063
IK4007287	10064
IK4007288	10065
IK4007289	10066
IK4007290	10067
IK4007291	10068
IK4007292	10069

IK4007293	10070
IK4007294	10071
IK4007295	10072
IK4007296	10073
IK4007297	10074
IK4007298	10075
IK4007299	10076
IK4007300	10077
IK4007301	10078
IK4007302	10079
IK4007303	10080
IK4007304	10081
IK4007317	10082
IK4009278	10083
IK4009279	10084
IK4009280	10085
IK4009281	10086
IK4009282	10087
IK4009283	10088
IK4009290	10089
IK4009291	10090
IK4009292	10091
IK4009293	10092
IK4009294	10093
IK4009295	10094
IK4009296	10095
IK4009297	10096
IK4009298	10097
IK4009299	10098
IK4009300	10099
IK4009301	10100

IK4009302	10101
IK4009306	10102
IK4009316	10103
IK4009317	10104
IK4009318	10105
IK4009319	10106
IK4009320	10107
IK4011023	10108
IK4011024	10109
IK4011025	10110
IK4011026	10111
IK4011027	10112
IK4012092	10113
IK4014018	10114
IK4014019	10115
IK4022015	10116
IK4022016	10117
IK4022017	10118
IK4201028	10119
IK4201029	10120
IK4201030	10121
IK4305234	10122
IK4305235	10123
IK4305236	10124
IK4305237	10125
IK4305244	10126
IK4305245	10127
IK4305246	10128
IK4305247	10129
IK4305248	10130
IK4305252	10131

IK4305253	10132
IK4305254	10133
IK4306131	10134
IK4306278	10135
IK4306279	10136
IK4306280	10137
IK4306281	10138
IK4306282	10139
IK4306283	10140
IK4306284	10141
IK4306285	10142
IK4306286	10143
IK4306287	10144
IK4306288	10145
IK4306289	10146
IK4306290	10147
IK4306292	10148
IK4306294	10149
IK4306295	10150
IK4306296	10151
IK4306297	10152
IK4306298	10153
IK4306299	10154
IK4306300	10155
IK4306301	10156
IK4306305	10157
IK4306306	10158
IK4306307	10159
IK4306308	10160
IK4306309	10161
IK4306310	10162

IK4306311	10163
IK4306315	10164
IK4306317	10165
IK4306320	10166
IK4306323	10167
IK4306325	10168
IK4306326	10169
IK4306327	10170
IK4306329	10171
IK4306331	10172
IK4306334	10173
IK4306336	10174
IK4306338	10175
IK4306348	10176
IK4306349	10177
IK4306351	10178
IK4306352	10179
IK4306353	10180
IK4306354	10181
IK4306355	10182
IK4306356	10183
IK4306357	10184
IK4306358	10185
IK4306359	10186
IK4306360	10187
IK4306361	10188
IK4306362	10189
IK4306363	10190
IK4306364	10191
IK4306365	10192
IK4306366	10193

IK4306367	10194
IK4306368	10195
IK4306369	10196
IK4306370	10197
IK4306371	10198
IK4306372	10199
IK4306373	10200
IK4306374	10201
IK4306375	10202
IK4306376	10203
IK4306377	10204
IK4306378	10205
IK4306379	10206
IK4306380	10207
IK4306381	10208
IK4306382	10209
IK4306383	10210
IK4306384	10211
IK4306385	10212
IK4306386	10213
IK4306387	10214
IK4306388	10215
IK4306389	10216
IK4306390	10217
IK4306391	10218
IK4306392	10219
IK4306393	10220
IK4306394	10221
IK4306395	10222
IK4306396	10223
IK4306397	10224

IK4306398	10225
IK4306399	10226
IK4306400	10227
IK4306401	10228
IK4306402	10229
IK4306403	10230
IK4306404	10231
IK4306405	10232
IK4306406	10233
IK4306410	10234
IK4306411	10235
IK4500097	10236
IK4500098	10237
IK4500099	10238
IK4500100	10239
IK4500109	10240
IK4500110	10241
IK4500111	10242
IK4500112	10243
IK4500113	10244
IK4500114	10245
IK4500115	10246
IK4500116	10247
IK4500135	10248
IK4500136	10249
IK4500137	10250
IK4500138	10251
IK4500139	10252
IK4500140	10253
IK4500141	10254
IK4500142	10255

IK4500143	10256
IK4500144	10257
IK4500145	10258
IK4500146	10259
IK4500147	10260
MsgQueueFull	10261
MsgQueueHighThreshold	10262
MsgQueueLowThreshold	10263
WmmLSS_cpiDropMGAllocConnReq	10264
WmmLSS_logRotateThreshold	10265
WmmLSS_serviceCFGDataTimestampError	10266
FTPLoginMaxAttempts	10267
TransportServerDegrade	10268
SubMngdHostOverride	10269
SubMngdHostCreationFail	10270
AuxDbCannotStart	10271
WMMSnapshotException	10272
AaStatTcaCfgThrshCross	9634
AaStatTcaFilterThrshCross	9635
AaStatTcaFltrEntryThrshCross	9636
AaStatTcaPolicerThrshCross	9637
AuxDbCannotRollbackToLastGoodEpoch	9638
DiamMessageDropped	9639
FRQSLTMISMATCH	9640
OCCPCR	9641
OCCPMJ	9642
OCCPMN	9643
PowerSupplyAcFailure	9644
PowerSupplyDcFailure	9645
PowerSupplyOverTemperature	9646
IsisPrefixLimitWarning	9647

IK8000105	9648
IK8000114	9649
IK8000116	9650
IK8000125	9651
IK8000190	9652
IK8000191	9653
IK8000192	9654
IK8000193	9655
IK8000194	9656
IK8000195	9657
IK8000196	9658
IK8000197	9659
IK8000199	9660
IK8000200	9661
IK8000201	9662
IK8000550	9663
IK8000551	9664
IK8000552	9665
IK8000553	9666
IK8000554	9667
IK8000555	9668
IK8000556	9669
IK8000557	9670
IK8000558	9671
IK8000559	9672
IK8000560	9673
IK8000561	9674
IK8000566	9675
IK8000567	9676
IK8000568	9677
IK8000569	9678

IK8000570	9679
IK8000571	9680
IK8000572	9681
IK8000573	9682
IK8000574	9683
IK8000575	9684
IK8000576	9685
IK8000577	9686
IK8000578	9687
IK8000579	9688
IK8000580	9689
IK8000581	9690
IK8000582	9691
IK8000583	9692
IK8000584	9693
IK8000585	9694
IK8000586	9695
IK8000587	9696
IK8000588	9697
IK8000589	9698
IK8000590	9699
IK8000591	9700
IK8000592	9701
IK8000593	9702
IK8000594	9703
IK8000595	9704
IK8000596	9705
IK8000597	9706
IK8000598	9707
IK8000599	9708
IK8000600	9709

IK8000601	9710
IK8000602	9711
IK8000603	9712
IK8000604	9713
IK8000605	9714
IK8000606	9715
IK8000607	9716
IK8000608	9717
IK8000609	9718
IK8000610	9719
IK8000611	9720
IK8000612	9721
IK8000613	9722
IK8020100	9723
IK8020101	9724
IK8020102	9725
IK8020103	9726
IK8020104	9727
IK8020105	9728
IK8020106	9729
IK8020107	9730
IK8020108	9731
IK8020109	9732
IK8020110	9733
IK8020111	9734
IK8020112	9735
IK8020113	9736
IK8020114	9737
IK8020115	9738
IK8020116	9739
IK8020117	9740

IK8020118	9741
IK8020119	9742
IK8020120	9743
IK8020121	9744
IK8020122	9745
IK8020123	9746
IK8020124	9747
IK8020125	9748
IK8020126	9749
IK8020127	9750
IK8020128	9751
IK8020129	9752
IK8020130	9753
IK8020131	9754
IK8020132	9755
IK8020133	9756
IK8020134	9757
IK8020135	9758
IK8020136	9759
IK8020137	9760
IK8020138	9761
IK8020139	9762
IK8020140	9763
IK8020141	9764
IK8020142	9765
IK8020143	9766
IK8020144	9767
IK8020145	9768
IK8020146	9769
IK8020147	9770
IK8020148	9771

IK8020149	9772
IK8020150	9773
IK8020205	9774
IK8100520	9775
IK8100521	9776
IK8100522	9777
IK8100523	9778
IK8100524	9779
IK8100525	9780
IK8100526	9781
IK8100527	9782
IK8100528	9783
IK8100529	9784
IK8100530	9785
IK8100531	9786
IK8100532	9787
IK8100533	9788
IK8100534	9789
IK8360000	9790
IK8360001	9791
IK8360002	9792
IK8360003	9793
IK8360004	9794
IK8360005	9795
IK8360006	9796
IK8360007	9797
IK8360505	9798
IK8360506	9799
IK8360507	9800
IK8361482	9801
IK8361484	9802

IK8361486	9803
IK8361508	9804
IK8361510	9805
IK8361513	9806
IK8361518	9807
IK8361523	9808
IK8361530	9809
IK8361533	9810
IK8361537	9811
IK8361540	9812
IK8361560	9813
IK8361573	9814
IK8361591	9815
IK8361602	9816
IK8361605	9817
IK8361612	9818
IK8361621	9819
IK8361625	9820
IK8361629	9821
IK8361635	9822
IK8361644	9823
IK8361648	9824
IK8361652	9825
IK8361654	9826
IK8361660	9827
IK8361663	9828
IK8362784	9829
IK8362791	9830
IK8362792	9831
IK8362795	9832
IK8362802	9833

IK8362837	9834
IK8362841	9835
IK8362843	9836
IK8362847	9837
IK8362849	9838
IK8362860	9839
IK8362863	9840
IK8362868	9841
IK8362869	9842
IK8362874	9843
IK8362875	9844
IK8362876	9845
IK8362877	9846
IK8362878	9847
IK8362879	9848
IK8362880	9849
IK8362882	9850
IK8362886	9851
IK8362887	9852
IK8362888	9853
IK8362891	9854
IK8362901	9855
IK8362908	9856
IK8362909	9857
IK8362911	9858
IK8362931	9859
IK8362932	9860
IK8362943	9861
IK8362944	9862
IK8362962	9863
IK8362964	9864

IK8362968	9865
IK8362990	9866
IK8362993	9867
IK8362994	9868
IK8362996	9869
IK8362999	9870
IK8363000	9871
IK8363002	9872
IK8363003	9873
IK8363004	9874
IK8363007	9875
IK8363008	9876
IK8363010	9877
IK8363012	9878
IK8363013	9879
IK8363018	9880
IK8363026	9881
IK8363027	9882
IK8363028	9883
IK8363029	9884
IK8363031	9885
IK8363033	9886
IK8363034	9887
IK8363036	9888
IK8363038	9889
IK8363039	9890
IK8363041	9891
IK8363043	9892
IK8363045	9893
IK8363046	9894
IK8363048	9895

IK8363050	9896
IK8363052	9897
IK8363054	9898
IK8363056	9899
IK8363059	9900
IK8363109	9901
IK8363110	9902
IK8363115	9903
IK8363116	9904
IK8363117	9905
IK8363120	9906
IK8363133	9907
IK8363136	9908
IK8363148	9909
IK8363157	9910
IK8363248	9911
IK8451048	9912
IK8451049	9913
IK8451050	9914
IK8452284	9915
IK8452443	9916
IK8452444	9917
IK8452462	9918
IK8452464	9919
IK8452468	9920
IK8452490	9921
IK8452493	9922
IK8452494	9923
IK8452496	9924
IK8452499	9925
IK8452500	9926

IK8452502	9927
IK8452503	9928
IK8452504	9929
IK8452507	9930
IK8452508	9931
IK8452510	9932
IK8452512	9933
IK8452513	9934
IK8452518	9935
IK8452526	9936
IK8452527	9937
IK8452528	9938
IK8452529	9939
IK8452531	9940
IK8452533	9941
IK8452534	9942
IK8452536	9943
IK8452538	9944
IK8452539	9945
IK8452541	9946
IK8452543	9947
IK8452545	9948
IK8452546	9949
IK8452548	9950
IK8452550	9951
IK8452552	9952
IK8452554	9953
IK8452556	9954
IK8454295	9955
IK8510011	9956
IK8510012	9957

IK8510013	9958
IK8552638	9959
IK8590015	9960
IK8590016	9961
IK8590017	9962
IK8590018	9963
IK8590019	9964
IK8590020	9965
IK8590021	9966
IK8590022	9967
IK8590023	9968
IK8590024	9969
IK8590025	9970
IK8590026	9971
IK8590027	9972
IK8690020	9973
IK8690021	9974
IK8690022	9975
IK8690023	9976
IK8690024	9977
IK8690025	9978
IK8690026	9979
IK8690027	9980
IK8690028	9981
IK8690029	9982
IK8690030	9983
IK8690031	9984
IK8690032	9985
IK8690033	9986
IK8690034	9987
IK8690035	9988

IK8690036	9989
IK8690037	9990
IK8690038	9991
IK8690039	9992
IK8690040	9993
IK8690041	9994
IK8690042	9995
IK8690043	9996
IK8690044	9997
IK8705940	9998
IK8752284	9999

2 1830 PSS (PSS-36 OCS, PSS-64 OCS)

2.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 2-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 2-2 ActiveFailedCrossConnectionProblem

Alarm	Attributes	Applicable major release
Name: ActiveFailedCrossConnectionProblem (8213) Type: communicationsAlarm Package: gmpls.ActiveFailedCrossConnectionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedCrossConnection-Problem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has failed due to a cross-connection problem. As a result, the system tries to establish a backup path in order to reroute the traffic.		
Remedial action: Not Available.		

Table 2-3 ActiveFailedEndpointFailure

Alarm	Attributes	Applicable major release
Name: ActiveFailedEndpointFailure (8214) Type: communicationsAlarm Package: gmpls.ActiveFailedEndpointFailure Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedEndpointFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when LSP drop port(s) at A-End and/or Z-End has a transmission alarm.		
Remedial action: Not Available.		

Table 2-4 ActiveFailedPreemption

Alarm	Attributes	Applicable major release
Name: ActiveFailedPreemption (8215) Type: communicationsAlarm Package: gmpls.ActiveFailedPreemption Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedPreemption	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has been preempted by another control plane service with a higher priority. As a result, the system tries to establish a backup path for the preempted service.		
Remedial action: Not Available.		

Table 2-5 ActiveFailedTransmissionProblem

Alarm	Attributes	Applicable major release
Name: ActiveFailedTransmissionProblem (8216) Type: communicationsAlarm Package: gmpls.ActiveFailedTransmissionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedTransmission-Problem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has failed due to a transmission problem. As a result, the system tries to establish a backup path in order to reroute the traffic.		
Remedial action: Not Available.		

Table 2-6 ActiveFailedUnprotected

Alarm	Attributes	Applicable major release
Name: ActiveFailedUnprotected (8217) Type: communicationsAlarm Package: gmpls.ActiveFailedUnprotected Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedUnprotected	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised an unprotected LSP has failed.		
Remedial action: Not Available.		

Table 2-7 ActiveLoopback

Alarm	Attributes	Applicable major release
Name: ActiveLoopback (8074) Type: communicationsAlarm Package: optical.ActiveLoopback Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ACTLPBK	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the associated facility has a loopback activated at the near end.		
Remedial action: The associated facility has a loopback activated at the near end.		

Table 2-8 AddPowerControlFailure

Alarm	Attributes	Applicable major release
Name: AddPowerControlFailure (4422) Type: equipmentAlarm Package: equipment.AddPowerControlFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mtcssurv Applicable probable causes: • Mtcssurv • MTCESURV	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Add power control failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-9 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 2-10 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 2-11 AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: AlarmIndicationSignal (8075) Type: communicationsAlarm Package: optical.AlarmIndicationSignal Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Alarm Indication Signal detected.		

Table 2-11 AlarmIndicationSignal (continued)

Alarm	Attributes	Applicable major release
Remedial action: Alarm Indication Signal detected.		

Table 2-12 ApplPersonelAttnRequired

Alarm	Attributes	Applicable major release
Name: ApplPersonelAttnRequired (5602) Type: equipmentAlarm Package: equipment.ApplPersonelAttnRequired Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APPLPAN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when application on a circuit pack needs personal assistance.		
Remedial action: Application on Circuitpack needs personal assistance.Details Please See User Manual		

Table 2-13 ApsSwitchedToWork

Alarm	Attributes	Applicable major release
Name: ApsSwitchedToWork (1977) Type: communicationsAlarm Package: equipment.ApsSwitchedToWork Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WkSwBk	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic switch to working is detected.		
Remedial action: Please refer section WKSWBK (Automatic switch to working) in 1830 Troubleshooting guide for detailed corrective action.		

Table 2-14 ApsWorkingForceSwitchedBackToWorking

Alarm	Attributes	Applicable major release
Name: ApsWorkingForceSwitchedBackToWorking (4432) Type: communicationsAlarm Package: equipment.ApsWorkingForceSwitchedBackToWorking Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdWkSwBk Applicable probable causes: • FrcdWkSwBk • FrcdWkSwBkVTS1 • FrcdWkSwBkVTS2 • FrcdWkSwBkVTS3 • FrcdWkSwBkVTS4 • FrcdWkSwBkVTS5 • FrcdWkSwBkVTS6 • FrcdWkSwBkVTS7 • FrcdWkSwBkVTS8 • FrcdWkSwBkVTS9 • FrcdWkSwBkVTS10	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to working is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-15 ApsWorkingForceSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingForceSwitchedToProtect (4433) Type: communicationsAlarm Package: equipment.ApsWorkingForceSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdWkSwPr Applicable probable causes: • FrcdWkSwPr • FrcdWkSwPrVTS1 • FrcdWkSwPrVTS2 • FrcdWkSwPrVTS3 • FrcdWkSwPrVTS4 • FrcdWkSwPrVTS6 • FrcdWkSwPrVTS7 • FrcdWkSwPrVTS8 • FrcdWkSwPrVTS9 • FrcdWkSwPrVTS10	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to protection is detected.		

Table 2-15 ApsWorkingForceSwitchedToProtect (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-16 ApsWorkingManualSwitchedBackToWorking

Alarm	Attributes	Applicable major release
Name: ApsWorkingManualSwitchedBackToWorking (4434) Type: communicationsAlarm Package: equipment.ApsWorkingManualSwitchedBackToWorking Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManWkSwBk Applicable probable causes: • ManWkSwBk • ManWkSwBkVTS1 • ManWkSwBkVTS2 • ManWkSwBkVTS3 • ManWkSwBkVTS4 • ManWkSwBkVTS5 • ManWkSwBkVTS6 • ManWkSwBkVTS7 • ManWkSwBkVTS8 • ManWkSwBkVTS9 • ManWkSwBkVTS10	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manual switch to working is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-17 ApsWorkingManualSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingManualSwitchedToProtect (4435) Type: communicationsAlarm Package: equipment. ApsWorkingManualSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManWkSwPr Applicable probable causes: • ManWkSwPr • ManWkSwPrVTS1 • ManWkSwPrVTS2 • ManWkSwPrVTS3 • ManWkSwPrVTS4 • ManWkSwPrVTS5 • ManWkSwPrVTS6 • ManWkSwPrVTS7 • ManWkSwPrVTS8 • ManWkSwPrVTS9 • ManWkSwPrVTS10	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manual switch to protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-18 ApsWorkingSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingSwitchedToProtect (4436) Type: communicationsAlarm Package: equipment.ApsWorkingSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WkSwPr Applicable probable causes: • WkSwPr • WkSwPrVTS1 • WkSwPrVTS2 • WkSwPrVTS3 • WkSwPrVTS4 • WkSwPrVTS5 • WkSwPrVTS6 • WkSwPrVTS7 • WkSwPrVTS8 • WkSwPrVTS9 • WkSwPrVTS10	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 2-18 ApsWorkingSwitchedToProtect (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Automatic switch to protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-19 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 2-20 AssymmetricalLANConnection

Alarm	Attributes	Applicable major release
Name: AssymmetricalLANConnection (5603) Type: equipmentAlarm Package: equipment.AssymmetricalLANConnection Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LANASYM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf LAN Cables are asymmetrical connected.		
Remedial action: Check the LAN Connection		

Table 2-21 AutomaticInService

Alarm	Attributes	Applicable major release
Name: AutomaticInService (8076) Type: communicationsAlarm Package: optical.AutomaticInService Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AINS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic in Service State detected.		
Remedial action: Automatic in Service State.		

Table 2-22 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 2-23 BackupUnavailable

Alarm	Attributes	Applicable major release
Name: BackupUnavailable (8218) Type: communicationsAlarm Package: gmpls.BackupUnavailable Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackupUnavailable	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is no inactive backup path is available. In case of failures, SBR will be used. This alarm is only relevant for LSPs with GR service type.		
Remedial action: Not Available.		

Table 2-24 BackwardDefectIndication

Alarm	Attributes	Applicable major release
Name: BackwardDefectIndication (4444) Type: communicationsAlarm Package: equipment.BackwardDefectIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Bdi Applicable probable causes: • Bdi • BdiOdu • BackwardDefectIndicationEgress • BDIS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Backward Defect Indication - OTU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-25 BackwardDefectIndicationEgress

Alarm	Attributes	Applicable major release
Name: BackwardDefectIndicationEgress (4914) Type: communicationsAlarm Package: equipment.BackwardDefectIndicationEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackwardDefectIndicationEgress Applicable probable causes: • BackwardDefectIndicationEgress • BDIP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Backward Defect Indication Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-26 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		

Table 2-26 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 2-27 BITSAIS

Alarm	Attributes	Applicable major release
Name: BITSAIS (4440) Type: communicationsAlarm Package: equipment.BITSAIS Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSAIS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS is detected is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-28 BITSLof

Alarm	Attributes	Applicable major release
Name: BITSLof (4441) Type: communicationsAlarm Package: equipment.BITSLof Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSLof	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-29 BITSLos

Alarm	Attributes	Applicable major release
Name: BITSLos (4442) Type: communicationsAlarm Package: equipment.BITSLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSLos	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		

Table 2-29 BITSLos (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-30 BITSMAN

Alarm	Attributes	Applicable major release
Name: BITSMAN (4443) Type: communicationsAlarm Package: equipment.BITSMAN Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSMAN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Logic removal of the BITS port is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-31 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 2-32 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 2-33 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 2-34 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 2-35 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 2-36 ColorViolation (gmpls)

Alarm	Attributes	Applicable major release
Name: ColorViolation (5562) Type: communicationsAlarm Package: gmpls.ColorViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ColorViolation	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route of the LSP breaks the color constraints regarding the specified include or exclude colors.		
Remedial action: Not Available.		

Table 2-37 CommunicationLoss

Alarm	Attributes	Applicable major release
Name: CommunicationLoss (5605) Type: equipmentAlarm Package: equipment.CommunicationLoss Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CONTCOMFLC Applicable probable causes: • CONTCOMFLC • CONTCOMMTX • CONTCOMQ1 • CONTCOMQ2 • CONTCOMQ3 • CONTCOMQ4	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Inter Card Communication Failure .		
Remedial action: Communication Loss happened interconnected Shelf/Circuitpack		

Table 2-38 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 2-39 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 2-39 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 2-40 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 2-41 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 2-42 CriticalTemperatureDetected

Alarm	Attributes	Applicable major release
Name: CriticalTemperatureDetected (5606) Type: environmentalAlarm Package: equipment.CriticalTemperatureDetected Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CRITICALTEMP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the temperature exceeded Critical Threshold.		
Remedial action: The NE has detected internal temperatures which are above critical. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 2-43 CsfGfpOut

Alarm	Attributes	Applicable major release
Name: CsfGfpOut (4458) Type: communicationsAlarm Package: equipment.CsfGfpOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CsfGfpOut Applicable probable causes: • CsfGfpOut • GFPCSF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Client Signal Fail detected on the GFP is detected.		
Remedial action: Refer Procedure: Clear Client Signal Failure (GFP) in 1830 Troubleshooting guide.		

Table 2-44 CsfOduOut

Alarm	Attributes	Applicable major release
Name: CsfOduOut (4459) Type: communicationsAlarm Package: equipment.CsfOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CsfOduOut Applicable probable causes: • CsfOduOut • ODUCSF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Client Signal Fail detected on the ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-45 DatabaseBackup

Alarm	Attributes	Applicable major release
Name: DatabaseBackup (8063) Type: equipmentAlarm Package: netw.DatabaseBackup Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DBBACKUP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when database backup is running.		
Remedial action: Database backup is running.		

Table 2-46 DatabaseBackupFailure

Alarm	Attributes	Applicable major release
Name: DatabaseBackupFailure (8064) Type: equipmentAlarm Package: netw.DatabaseBackupFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DBF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when creation of local backup database failed.		
Remedial action: Creation of local backup database failed.		

Table 2-47 DatabaseRestore

Alarm	Attributes	Applicable major release
Name: DatabaseRestore (8065) Type: equipmentAlarm Package: netw.DatabaseRestore Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DBRESTORE	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when database restore is running.		
Remedial action: Database restore is running.		

Table 2-48 DatabaseRestoreFailure

Alarm	Attributes	Applicable major release
Name: DatabaseRestoreFailure (8066) Type: equipmentAlarm Package: netw.DatabaseRestoreFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DRF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when restoration of local backup database failed.		
Remedial action: Restoration of local backup database failed.		

Table 2-49 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 2-50 DPRDegraded

Alarm	Attributes	Applicable major release
Name: DPRDegraded (8219) Type: communicationsAlarm Package: gmpls.DPRDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the OSPF routing protocol, which is used for data plane routing (DPR) between the adjacent nodes, is not fully operational.		
Remedial action: Not Available.		

Table 2-51 DPRDown

Alarm	Attributes	Applicable major release
Name: DPRDown (8220) Type: communicationsAlarm Package: gmpls.DPRDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication to the adjacent node for OSPF data plane routing is not working.		
Remedial action: Not Available.		

Table 2-52 DPRNetworkVersionMismatch

Alarm	Attributes	Applicable major release
Name: DPRNetworkVersionMismatch (8221) Type: communicationsAlarm Package: gmpls.DPRNetworkVersionMismatch Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRNetworkVersionMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the GMRE active network version of the adjacent node does not match the active network version of the local node.		
Remedial action: Not Available.		

Table 2-53 DuplexImpaired

Alarm	Attributes	Applicable major release
Name: DuplexImpaired (8373) Type: equipmentAlarm Package: equipment.DuplexImpaired Raised on class: equipment.CardSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DXIMPAIRED	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The FLC or MTX EQP group in the main or extension shelf has a group state unequal to NOREQ (being either degraded by equipment failures or forced by commands or recovery/alignment pending or in simplex operation) .		
Remedial action: This alarm indicates that the FLC or MTX EQP group in the main or extension shelf has a group state unequal to NOREQ (being either degraded by equipment failures or forced by commands or recovery/alignment pending or in simplex operation)		

Table 2-54 DuplicateDPNodeIP

Alarm	Attributes	Applicable major release
Name: DuplicateDPNodeIP (8974) Type: configurationAlarm Package: netw.DuplicateDPNodeIP Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: duplicateDPNodeIP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects that the DP Node IP Address is being used by multiple GMRE Sub-Nodes. Per the GMRE guide, the DP Node IP Address has to be unique network-wide. To prevent discovery of a misconfigured network, the GMPLS entities are not discovered in SAM when this alarm gets raised. Please reconfigure before attempting to add this node to an ASON domain.		
Remedial action: The DP Node IP Address on one of the Sub-Nodes on this NE is not unique within the ASON domain network. Please reconfigure the IP address before attempting to add this node to an ASON domain.		

Table 2-55 DuplicateShelfId

Alarm	Attributes	Applicable major release
Name: DuplicateShelfId (5607) Type: equipmentAlarm Package: equipment.DuplicateShelfId Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DUPSHELFID	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there are two or more extension shelves with same Shelf ID		
Remedial action: Remove the Shelf and Reconfigure with correct Id.		

Table 2-56 Ebero

Alarm	Attributes	Applicable major release
Name: Ebero (3348) Type: communicationsAlarm Package: equipment.Ebero Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EBERO Applicable probable causes: • EBERO • EBER	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical supervision channel excessive BER is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-57 EOCFailure

Alarm	Attributes	Applicable major release
Name: EOCFailure (8077) Type: communicationsAlarm Package: optical.EOCFailure Raised on class: optical.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EOC	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Embedded Operations Channel failure occurs and no adjacencies are formed.		
Remedial action: Please refer EOC in 1830 Troubleshooting guide for detailed corrective procedure.		

Table 2-58 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 2-59 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 2-60 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 2-61 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 2-62 EquipmentRemovalWhenNoProtection

Alarm	Attributes	Applicable major release
Name: EquipmentRemovalWhenNoProtection (5608) Type: equipmentAlarm Package: equipment. EquipmentRemovalWhenNoProtection Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MAN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Logical Removal of Equipment where no protection mate is available.		
Remedial action: Reconfigure the Main Circuitpack		

Table 2-63 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 2-64 ExtensionHeaderMismatchGFP

Alarm	Attributes	Applicable major release
Name: ExtensionHeaderMismatchGFP (8110) Type: communicationsAlarm Package: oth.ExtensionHeaderMismatchGFP Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GFPEXM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Extension Header Mismatch on the ODUPTF detected. Always Service affecting.		
Remedial action: Extension Header Mismatch on the ODUPTF.		

Table 2-65 ExternalLANFailure

Alarm	Attributes	Applicable major release
Name: ExternalLANFailure (8078) Type: communicationsAlarm Package: optical.ExternalLANFailure Raised on class: optical.ControlNetworkSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EXTLANFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Link down on an external LAN interface (management LAN or shelf interconnection LAN) is detected.		
Remedial action: Link down on an external LAN interface (management LAN or shelf interconnection LAN).		

Table 2-66 FacilityLoopbackConfigured (oth)

Alarm	Attributes	Applicable major release
Name: FacilityLoopbackConfigured (8380) Type: communicationsAlarm Package: oth.FacilityLoopbackConfigured Raised on class: oth.Otuk	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FacilityLoopbackConfigured	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Facility Loopback is configured on Facility.		
Remedial action: To clear the condition, disable Facility Loopback configured on OTUk.		

Table 2-67 FacilityManualRemoval

Alarm	Attributes	Applicable major release
Name: FacilityManualRemoval (8079) Type: communicationsAlarm Package: optical.FacilityManualRemoval Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MAN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when related facility is manually taken out of service while it has condition on it.		
Remedial action: Related facility is manually taken out of service.		

Table 2-68 FailureOfProtocolInconsistent

Alarm	Attributes	Applicable major release
Name: FailureOfProtocolInconsistent (8111) Type: communicationsAlarm Package: oth.FailureOfProtocolInconsistent Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FOPINCON	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the received APS protocol is not stable.		
Remedial action: Failure Of Protocol - Inconsistent.		

Table 2-69 FailureOfProtocolNoResponse

Alarm	Attributes	Applicable major release
Name: FailureOfProtocolNoResponse (8112) Type: communicationsAlarm Package: oth.FailureOfProtocolNoResponse Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FOPNR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when detected protocol interaction problem from comparing the Entity ID fields of the transmitted and the received APS protocol.		
Remedial action: Failure Of Protocol - No Response.		

Table 2-70 FailureOfProtocolOperationMismatch

Alarm	Attributes	Applicable major release
Name: FailureOfProtocolOperationMismatch (8113) Type: communicationsAlarm Package: oth.FailureOfProtocolOperationMismatch Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FOPOM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when detected protocol provisioning mismatch from comparing R bits (=" revertive / non-revertive) of the transmitted and the received APS protocol."		
Remedial action: Failure Of Protocol - Operation Mismatch.		

Table 2-71 FailureOfProtocolProvisioningMismatch

Alarm	Attributes	Applicable major release
Name: FailureOfProtocolProvisioningMismatch (8114) Type: communicationsAlarm Package: oth.FailureOfProtocolProvisioningMismatch Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FOPPM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when detected protocol provisioning mismatch from comparing A and B bits (=" protocol usage and 1+1 / 1:n architecture) of the transmitted and the received APS protocol. ."		
Remedial action: Failure Of Protocol - Provisioning Mismatch.		

Table 2-72 FailureOfProtocolSwitchMismatch

Alarm	Attributes	Applicable major release
Name: FailureOfProtocolSwitchMismatch (8115) Type: communicationsAlarm Package: oth.FailureOfProtocolSwitchMismatch Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FOPSM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when detected protocol provisioning mismatch from comparing D bits (=" uni- / bi-directional switching) of the transmitted and the received APS protocol."		
Remedial action: Failure Of Protocol - Switch Mismatch.		

Table 2-73 FastPhotonicRestModeMismatch

Alarm	Attributes	Applicable major release
Name: FastPhotonicRestModeMismatch (10280) Type: equipmentAlarm Package: gmpls.FastPhotonicRestModeMismatch Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FastPhotonicRestModeMis-match	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an inconsistency in provisioning of the FastPhotonicRestoration parameter is detected.		
Remedial action: Reconfigure FastPhotonicRestoration parameter.		

Table 2-74 FilterBlocked

Alarm	Attributes	Applicable major release
Name: FilterBlocked (5610) Type: equipmentAlarm Package: equipment.FilterBlocked Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FLTBLKD	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when air filter of the shelf gets blocked		
Remedial action: Filter on the Shelf is Blocked, remove the filter and repair		

Table 2-75 FilterClogged

Alarm	Attributes	Applicable major release
Name: FilterClogged (5611) Type: equipmentAlarm Package: equipment.FilterClogged Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FLTCLOGCRIT Applicable probable causes: • FLTCLOGCRIT • FLTCLOGHIGH	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when air filter of the shelf gets clogged		
Remedial action: Filter on the Shelf is Clogged remove the filter and repair		

Table 2-76 FilterMissing

Alarm	Attributes	Applicable major release
Name: FilterMissing (5612) Type: equipmentAlarm Package: equipment.FilterMissing Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FLTMISS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when air filter of the shelf is missing		
Remedial action: Filter is missing on the shelf, Reinsert the Filter		

Table 2-77 FirmwareUpgradeFailure

Alarm	Attributes	Applicable major release
Name: FirmwareUpgradeFailure (5613) Type: equipmentAlarm Package: equipment.FirmwareUpgradeFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FWUPGRADEFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised for Firmware Upgrade Fail .		
Remedial action: Firm Ware Upgrade Failed. Re do the firmware upgrade again		

Table 2-78 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 2-79 FrcdSwTimRef

Alarm	Attributes	Applicable major release
Name: FrcdSwTimRef (3922) Type: equipmentAlarm Package: optical.FrcdSwTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdSwTimRef	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to a timing reference is detected.		
Remedial action: Clear force switch.		

Table 2-80 FrngSync

Alarm	Attributes	Applicable major release
Name: FrngSync (3722) Type: equipmentAlarm Package: equipment.FrngSync Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrngSync	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is raised when the system clock is in free-running mode.		
Remedial action: The alarm is raised when system clock in free running mode.Proceed to Procedure -Clear System clock is in free running synchronization mode alarm in 1830 Troubleshooting guide.		

Table 2-81 FuseFailure

Alarm	Attributes	Applicable major release
Name: FuseFailure (5614) Type: equipmentAlarm Package: equipment.FuseFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FA	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised for Fuse Alarm .		
Remedial action: Fuse Alarm, Check the Fuse in the Shelf		

Table 2-82 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 2-83 GfpLofOut

Alarm	Attributes	Applicable major release
Name: GfpLofOut (4488) Type: communicationsAlarm Package: equipment.GfpLofOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpLofOut Applicable probable causes: • GfpLofOut • GFPLOF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Loss of GFP alignment is detected.		
Remedial action: Refer Procedure : Clear Loss of GFP alignment in 1830 Troubleshooting guide.		

Table 2-84 GmreDegraded

Alarm	Attributes	Applicable major release
Name: GmreDegraded (8222) Type: equipmentAlarm Package: gmpls.GmreDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is not fully operational.		
Remedial action: Not Available.		

Table 2-85 GmreInAutomaticRestorationDisabledMode

Alarm	Attributes	Applicable major release
Name: GmreInAutomaticRestorationDisabledMode (8223) Type: equipmentAlarm Package: gmpls. GmreInAutomaticRestorationDisabledMode Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreInAutomaticRestora-tionDisabledMode	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is set to manual restoration by operator.		
Remedial action: Not Available.		

Table 2-86 GmreInMigration

Alarm	Attributes	Applicable major release
Name: GmreInMigration (8224) Type: equipmentAlarm Package: gmpls.GmreInMigration Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreInMigration	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is in Migration.		
Remedial action: Not Available.		

Table 2-87 HardwareFailure

Alarm	Attributes	Applicable major release
Name: HardwareFailure (5615) Type: equipmentAlarm Package: equipment.HardwareFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HWFAIL Applicable probable causes: • HWFAIL • HWMCPF • HWSUSP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised for Hardware Failure .		
Remedial action: Hardware error is detected, replace the hardware.		

Table 2-88 HighTemperatureDetected

Alarm	Attributes	Applicable major release
Name: HighTemperatureDetected (5616) Type: environmentalAlarm Package: equipment.HighTemperatureDetected Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HIGHTEMP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the temperature exceeded High Threshold.		
Remedial action: High Temperature Detected,Check the Fan is working properly		

Table 2-89 HldOvrSync

Alarm	Attributes	Applicable major release
Name: HldOvrSync (3917) Type: equipmentAlarm Package: equipment.HldOvrSync Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HldOvrSync	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the system clock is in hold-over mode.		
Remedial action: Check all references.		

Table 2-90 InBandCommDegraded

Alarm	Attributes	Applicable major release
Name: InBandCommDegraded (8225) Type: communicationsAlarm Package: gmpls.InBandCommDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandCommDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a problem on at least one ECC channel of the ECC protection group. The ECC channel might be not protected anymore.		
Remedial action: Not Available.		

Table 2-91 InBandCommDown

Alarm	Attributes	Applicable major release
Name: InBandCommDown (8226) Type: communicationsAlarm Package: gmpls.InBandCommDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandCommDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP communication via the ECC protection group is not working.		
Remedial action: Not Available.		

Table 2-92 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 2-93 InHsWdx

Alarm	Attributes	Applicable major release
Name: InHsWdx (5619) Type: equipmentAlarm Package: equipment.InHsWdx Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INHSWDX	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when 1+1 equipment protection group is inhibited .		
Remedial action: A 1+1 equipment protection group is inhibited to switch. Use ALW-SWDX-EQPT TL1 Command		

Table 2-94 IntClockMiss

Alarm	Attributes	Applicable major release
Name: IntClockMiss (5620) Type: equipmentAlarm Package: equipment.IntClockMiss Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTCLOCKMISS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the clock signal generated by the specified MTX is not distributed internally.		
Remedial action: The clock signal generated by the specified MTXis not distributed internally.		

Table 2-95 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 2-96 InternalCommunicationFailure

Alarm	Attributes	Applicable major release
Name: InternalCommunicationFailure (5625) Type: equipmentAlarm Package: equipment.InternalCommunicationFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ECCCOMA Applicable probable causes: • ECCCOMA • ECCCOMB	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when internal Communication Failure Between FLC and ECC(A/B) .		
Remedial action: Internal Communication Failure		

Table 2-97 InternalLanDegrade

Alarm	Attributes	Applicable major release
Name: InternalLanDegrade (5626) Type: equipmentAlarm Package: equipment.InternalLanDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTLANDEGR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal LAN redundancy is degraded .		
Remedial action: Internal Lan Degrade, check the LAN Connectivity.		

Table 2-98 InternalLanFail

Alarm	Attributes	Applicable major release
Name: InternalLanFail (5627) Type: equipmentAlarm Package: equipment.InternalLanFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTLANFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal LAN connection is failed .		
Remedial action: Internal Lan Failure, Repair the LAN Connectivity		

Table 2-99 InternalPayLoadIntegrity

Alarm	Attributes	Applicable major release
Name: InternalPayLoadIntegrity (5628) Type: equipmentAlarm Package: equipment.InternalPayLoadIntegrity Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTERRA Applicable probable causes: • INTERRA • INTERRB	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Problem with Integrity of the internal payload .		
Remedial action: Internal PayLoad Integrity		

Table 2-100 InternalSynchSignal

Alarm	Attributes	Applicable major release
Name: InternalSynchSignal (5629) Type: equipmentAlarm Package: equipment.InternalSynchSignal Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTSYNCMISSA Applicable probable causes: • INTSYNCMISSA • INTSYNCMISSB	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal LAN connection is failed .		
Remedial action: Internal Synchronization Signal Generated by the MTX is corrupted		

Table 2-101 IPCPConnectionFailure

Alarm	Attributes	Applicable major release
Name: IPCPConnectionFailure (8080) Type: communicationsAlarm Package: optical.IPCPConnectionFailure Raised on class: optical.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPCPCONFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no IPCP connection could be established on an ECC provisioned for IP. The alarm is raised after 10 unsuccessful attempts to establish the IPCP.		
Remedial action: Please refer IPCPCONNFAIL in 1830 Troubleshooting guide for detailed corrective procedure.		

Table 2-102 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 2-103 LanLol

Alarm	Attributes	Applicable major release
Name: LanLol (4499) Type: communicationsAlarm Package: equipment.LanLol Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanLol Applicable probable causes: • LanLol • LOL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Link is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-104 LatchOpen

Alarm	Attributes	Applicable major release
Name: LatchOpen (5630) Type: equipmentAlarm Package: equipment.LatchOpen Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LATCHOPEN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one of the latches is not closed .		
Remedial action: Indicates that one of the latches are not closed.Close the Latch		

Table 2-105 LatencyViolation

Alarm	Attributes	Applicable major release
Name: LatencyViolation (8227) Type: communicationsAlarm Package: gmpls.LatencyViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LatencyViolation	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route of the LSP breaks the specified latency constraints.		
Remedial action: Not Available.		

Table 2-106 LckOut

Alarm	Attributes	Applicable major release
Name: LckOut (4500) Type: communicationsAlarm Package: equipment.LckOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LckOut Applicable probable causes: • LckOut • LCK	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Locked - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-107 LCPConnectionFailure

Alarm	Attributes	Applicable major release
Name: LCPConnectionFailure (8081) Type: communicationsAlarm Package: optical.LCPConnectionFailure Raised on class: optical.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LCPCONFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when communication over an ECC is not possible because the link control protocol(LCP) could not be established between the two ends of the link. The alarm is raised after 10 unsuccessful attempts to establish the LCP.		
Remedial action: Please refer LCPCONNFAIL in 1830 Troubleshooting guide for detailed corrective procedure.		

Table 2-108 LeftLanWronglyConnected

Alarm	Attributes	Applicable major release
Name: LeftLanWronglyConnected (5631) Type: equipmentAlarm Package: equipment.LeftLanWronglyConnected Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LANLEFTRING	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf neighbors are missing in left LAN.		
Remedial action: Left LAN is wrongly Connected. Check the LAN Connectivity		

Table 2-109 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 2-110 LinkDiversityViolation

Alarm	Attributes	Applicable major release
Name: LinkDiversityViolation (8228) Type: communicationsAlarm Package: gmpls.LinkDiversityViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LinkDiversityViolation	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no fully link-diverse backup route could be found for the current route of the LSP.		
Remedial action: Not Available.		

Table 2-111 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 2-112 LockOutOfProtection

Alarm	Attributes	Applicable major release
Name: LockOutOfProtection (8116) Type: communicationsAlarm Package: oth.LockOutOfProtection Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOCKOUTOFPR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Lock out of Protection facility detected.		
Remedial action: Lock out of Protection facility detected.		

Table 2-113 LockoutOfTimRef

Alarm	Attributes	Applicable major release
Name: LockoutOfTimRef (3923) Type: equipmentAlarm Package: optical.LockoutOfTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LockoutOfTimRef	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Lock out of a timing reference is detected.		
Remedial action: Check the timing reference quality and priority.		

Table 2-114 LockOutOfWorking

Alarm	Attributes	Applicable major release
Name: LockOutOfWorking (8117) Type: communicationsAlarm Package: oth.LockOutOfWorking Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOCKOUTWR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Lockout of working facility detected. The related normal traffic ODUn is not allowed to request usage of protection. .		
Remedial action: Lockout of working facility detected.		

Table 2-115 LOFLOM

Alarm	Attributes	Applicable major release
Name: LOFLOM (4496) Type: communicationsAlarm Package: equipment.LOFLOM Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOFLOM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU LOFLOM is detected.		
Remedial action: Refer Procedure : Clear Loss of Frame and Loss of Multiframe in 1830 Troubleshooting guide.		

Table 2-116 LogicalNodeNotReachable

Alarm	Attributes	Applicable major release
Name: LogicalNodeNotReachable (8229) Type: equipmentAlarm Package: gmpls.LogicalNodeNotReachable Raised on class: gmpls.SubNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LogicalNodeNotReachable	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Logical Node (OCS shelf) with the specified logical node ID is not reachable, that is , the communication to this OCS shelf is disturbed.		
Remedial action: Not Available.		

Table 2-117 LoI

Alarm	Attributes	Applicable major release
Name: LoI (4504) Type: communicationsAlarm Package: equipment.LoI Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoI	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Lane Alignment is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-118 LosOts

Alarm	Attributes	Applicable major release
Name: LosOts (3372) Type: communicationsAlarm Package: equipment.LosOts Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosOts Applicable probable causes: • LosOts • LOSOTS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OPS Input Loss of Signal is detected.		
Remedial action: Please refer LOS-P (Incoming Payload LOS) in 1830 Troubleshooting guide for detailed corrective action.		

Table 2-119 LossOfFrame (optical)

Alarm	Attributes	Applicable major release
Name: LossOfFrame (630) Type: communicationsAlarm Package: optical.LossOfFrame Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lof Applicable probable causes: • Lof • LOF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer 1830 PSS Node Maintenance manual for remedial action information.		

Table 2-120 LossOfMultiFrame (oth)

Alarm	Attributes	Applicable major release
Name: LossOfMultiFrame (3930) Type: communicationsAlarm Package: oth.LossOfMultiFrame Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Multiframe detected.		
Remedial action: Loss of Multiframe.		

Table 2-121 LossOfOPUMultiFrameIdentifier

Alarm	Attributes	Applicable major release
Name: LossOfOPUMultiFrameIdentifier (8118) Type: communicationsAlarm Package: oth.LossOfOPUMultiFrameIdentifier Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOOMFI	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of OPU MultiFrame Identifier detected.		
Remedial action: Loss of OPU MultiFrame Identifier.		

Table 2-122 LossOfSignal (optical)

Alarm	Attributes	Applicable major release
Name: LossOfSignal (631) Type: communicationsAlarm Package: optical.LossOfSignal Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los Applicable probable causes: • Los • LosP • LosOut • LosLdSig • LanLos • LOS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		

Table 2-122 LossOfSignal (optical) (continued)

Alarm	Attributes	Applicable major release
Remedial action: A receive port on one of the optical cards has detected a loss of signal. The LOS condition may be raised for the following reasons:1. a misconnected, damaged, or dirty fiber.2. the received power may not be within the acceptable range.The procedures in this section are as follows:1. LOS (Channel Absent Alarm) 2. LD Input LOS.3. CWR Input LOS.4. LOS (Loss of Signal.Please refer detailed section for each in 1830 Troubleshooting guide.		

Table 2-123 LossOfSync

Alarm	Attributes	Applicable major release
Name: LossOfSync (4510) Type: communicationsAlarm Package: equipment.LossOfSync Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lss Applicable probable causes: • Lss • LSS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of synchronization is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-124 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 2-125 Lssc

Alarm	Attributes	Applicable major release
Name: Lssc (5632) Type: equipmentAlarm Package: equipment.Lssc Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSSC	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the subsystem controlled by the equipment cannot be provisioned or supervised at the moment .		
Remedial action: The Subsystem controlled by the equipment cannot be provisioned or supervised at the moment		

Table 2-126 Lvco

Alarm	Attributes	Applicable major release
Name: Lvco (5633) Type: equipmentAlarm Package: equipment.Lvco Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LVCO	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the battery supervision detects low voltage .		
Remedial action: Battery supervision detects low voltage,Repair Battery		

Table 2-127 ManSwTimRef

Alarm	Attributes	Applicable major release
Name: ManSwTimRef (3925) Type: equipmentAlarm Package: optical.ManSwTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManSwTimRef	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manual switch to a timing reference is detected.		
Remedial action: Check the timing reference quality and priority.		

Table 2-128 ManSwToInt

Alarm	Attributes	Applicable major release
Name: ManSwToInt (3918) Type: equipmentAlarm Package: equipment.ManSwToInt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManSwToInt	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System clock forced to internal clock is detected.		
Remedial action: Clear the manual switch.		

Table 2-129 MaxHopViolation

Alarm	Attributes	Applicable major release
Name: MaxHopViolation (8230) Type: communicationsAlarm Package: gmpls.MaxHopViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxHopViolation	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route of the LSP breaks the specified maximum number of hops.		
Remedial action: Not Available.		

Table 2-130 Misc

Alarm	Attributes	Applicable major release
Name: Misc (5634) Type: equipmentAlarm Package: equipment.Misc Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MISC_1	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised standby CRU is not tracking the active CRU.		
Remedial action: Indicates that the standby CRU is not tracking the active CRU.		

Table 2-131 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 2-132 ModulesNotProvisioned

Alarm	Attributes	Applicable major release
Name: ModulesNotProvisioned (5635) Type: equipmentAlarm Package: equipment.ModulesNotProvisioned Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ABNORMAL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when module is available in a position but not provisioned.		
Remedial action: Card is Not Provisioned but available, Provision the Card		

Table 2-133 Msim

Alarm	Attributes	Applicable major release
Name: Msim (3377) Type: communicationsAlarm Package: equipment.Msim Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Msim	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Multiplex Structure Identifier Mismatch is detected.		

Table 2-133 Msim (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please follow the below steps to clear this alarm:\n 1. Check if there is a signal degraded alarm reported at OT Port. Perform the corrective action for clearing the alarms found.\n 2. After all degraded alarms are cleared retrieve the Digital Wrapper performance monitoring group by executing the following command on node CLI: "show interface card_type shelf slot L1 PM DW".\n 3. Check whether uncorrectable FEC bit errors are reported. If so, perform the action for clearing the signal degraded alarms.\n 4. After all signal degraded alarms are cleared and no uncorrectable bit errors are reported, check whether the input OTU signal MSI byte is compliant with received OT card settings.		

Table 2-134 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 2-135 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		

Table 2-135 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 2-136 NeNotReachable

Alarm	Attributes	Applicable major release
Name: NeNotReachable (8231) Type: equipmentAlarm Package: gmpls.NeNotReachable Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeNotReachable	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication between the GMRE and the managed NE is disturbed.		
Remedial action: Not Available.		

Table 2-137 NeUnavailable

Alarm	Attributes	Applicable major release
Name: NeUnavailable (8068) Type: equipmentAlarm Package: netw.NeUnavailable Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NEUNAVAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the whole system cannot be provisioned or supervised at the moment.		
Remedial action: The whole system cannot be provisioned or supervised at the moment.		

Table 2-138 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 2-139 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 2-140 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 2-140 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 2-141 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 2-142 NominalUnavailableCommunicationProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableCommunicationProblem (8232) Type: communicationsAlarm Package: gmpls. NominalUnavailableCommunicationProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableCommunicationProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed due to control plane problem.		
Remedial action: Not Available.		

Table 2-143 NominalUnavailableConfigurationProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableConfigurationProblem (8233) Type: communicationsAlarm Package: gmpls.NominalUnavailableConfigurationProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableConfigurationProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route is not active due to a wrong configuration (could be either node, link or label).		
Remedial action: Not Available.		

Table 2-144 NominalUnavailableIndeterminateProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableIndeterminateProblem (8234) Type: communicationsAlarm Package: gmpls.NominalUnavailableIndeterminateProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableIndeterminateProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed for no specific reason.		
Remedial action: Not Available.		

Table 2-145 NominalUnavailableReversionPreempt

Alarm	Attributes	Applicable major release
Name: NominalUnavailableReversionPreempt (8235) Type: communicationsAlarm Package: gmpls.NominalUnavailableReversionPreempt Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableReversionPreempt	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route is not active due to a resource currently being used by a lower priority LSP.		
Remedial action: Not Available.		

Table 2-146 NominalUnavailableTPBlocked

Alarm	Attributes	Applicable major release
Name: NominalUnavailableTPBlocked (8236) Type: communicationsAlarm Package: gmpls.NominalUnavailableTPBlocked Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableTP-Blocked	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal resources are blocked by higher priority traffic.		
Remedial action: Not Available.		

Table 2-147 NominalUnavailableTransmissionProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableTransmissionProblem (8237) Type: communicationsAlarm Package: gmpls. NominalUnavailableTransmissionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableTransmis-sionProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed due to data plane problem.		
Remedial action: Not Available.		

Table 2-148 NotAligned

Alarm	Attributes	Applicable major release
Name: NotAligned (5637) Type: equipmentAlarm Package: equipment.NotAligned Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DXNOTALGND	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when inactive entity of an 1+1 equipment Protection Group is not aligned .		
Remedial action: The inactive entity of an 1+1 equipment protection group is not aligned.		

Table 2-149 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 2-150 NTPServerIsNotReachable

Alarm	Attributes	Applicable major release
Name: NTPServerIsNotReachable (5636) Type: equipmentAlarm Package: equipment.NTPServerIsNotReachable Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOOSYNC	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no NTP Server is Reachable.		
Remedial action: NTP Server not reachable.Check the Status of NTP Server		

Table 2-151 OciOut

Alarm	Attributes	Applicable major release
Name: OciOut (4519) Type: communicationsAlarm Package: equipment.OciOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OciOut Applicable probable causes: • OciOut • OCI	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Open Connection Indication - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-152 OprTx

Alarm	Attributes	Applicable major release
Name: OprTx (3383) Type: communicationsAlarm Package: equipment.OprTx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprTx	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel power unstable is detected.		
Remedial action: This alarm is raised on cards with a Wavelength Tracker detect point when the power is outside of the provisioned power range. For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 2-153 OpticalOutputPowerUnachievable

Alarm	Attributes	Applicable major release
Name: OpticalOutputPowerUnachievable (4524) Type: communicationsAlarm Package: equipment. OpticalOutputPowerUnachievable Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprUnachieve	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel power unachievable is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-154 OpticalParameterFileError

Alarm	Attributes	Applicable major release
Name: OpticalParameterFileError (8238) Type: equipmentAlarm Package: gmpls.OpticalParameterFileError Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpticalParameterFileError	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the last downloaded file with optical feasibility target values (from the EPT) is not valid.		
Remedial action: Not Available.		

Table 2-155 OSPFAdjacencyFailure

Alarm	Attributes	Applicable major release
Name: OSPFAdjacencyFailure (8083) Type: communicationsAlarm Package: optical.OSPFAdjacencyFailure Raised on class: optical.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OSPFADJFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OSPF is enabled in active mode, but no adjacency is formed via the interface.		
Remedial action: Check the OSPF configuration on the peer NE/router of the alarmed interface, and verify whether the OSPF configuration settings at both ends of the link are compatible.		

Table 2-156 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 2-157 OutBandCommDegraded

Alarm	Attributes	Applicable major release
Name: OutBandCommDegraded (8239) Type: communicationsAlarm Package: gmpls.OutBandCommDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OutBandCommDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a problem on at least one out-of-band tunnel.		
Remedial action: Not Available.		

Table 2-158 OutBandCommDown

Alarm	Attributes	Applicable major release
Name: OutBandCommDown (8240) Type: communicationsAlarm Package: gmpls.OutBandCommDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OutBandCommDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP communication via the out-of-band tunnel is not working.		
Remedial action: Not Available.		

Table 2-159 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 2-160 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		

Table 2-160 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 2-161 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 2-162 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 2-163 PhysicalRemoval

Alarm	Attributes	Applicable major release
Name: PhysicalRemoval (5639) Type: equipmentAlarm Package: equipment.PhysicalRemoval Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IMPROPRMVL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when physical removal performed without logical removal .		
Remedial action: Physical Removal is done without logical removal, please issue RMV-EQPT- command before physically removing the equipment		

Table 2-164 PlmOduOut

Alarm	Attributes	Applicable major release
Name: PlmOduOut (4528) Type: communicationsAlarm Package: equipment.PlmOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PlmOduOut Applicable probable causes: • PlmOduOut • PLMP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Payload Mismatch Indication - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-165 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		

Table 2-165 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 2-166 PowerFailure

Alarm	Attributes	Applicable major release
Name: PowerFailure (5641) Type: equipmentAlarm Package: equipment.PowerFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PWR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a alarming equipment detects power failure.		
Remedial action: Power Failure Detected. Check the Power		

Table 2-167 PRCDRERR

Alarm	Attributes	Applicable major release
Name: PRCDRERR (5638) Type: equipmentAlarm Package: equipment.PRCDRERR Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PRCDRERR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a non compatible module inserted in to shelf.		
Remedial action: Not compatible module is inserted in to a shelf.Module is not consistent with HW slot/Sw assignment.Remove the Module.		

Table 2-168 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		

Table 2-168 PrimaryImageBootFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 2-169 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 2-170 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 2-171 ReadyToRevert (gmpls)

Alarm	Attributes	Applicable major release
Name: ReadyToRevert (5586) Type: communicationsAlarm Package: gmpls.ReadyToRevert Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReadyToRevert	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal resources are available again, and a reversion can be done.		
Remedial action: Not Available.		

Table 2-172 ReceiveTimingFailure

Alarm	Attributes	Applicable major release
Name: ReceiveTimingFailure (5643) Type: equipmentAlarm Package: equipment.ReceiveTimingFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RCVTIMFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a received timing signal internally failed to be sent.		
Remedial action: A received timing signal internally failed to be sent to the MTX Card.		

Table 2-173 RemoteFailureIndication

Alarm	Attributes	Applicable major release
Name: RemoteFailureIndication (4538) Type: communicationsAlarm Package: equipment.RemoteFailureIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanRfi	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Fault is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-174 RemoteInventoryMisMatch

Alarm	Attributes	Applicable major release
Name: RemoteInventoryMisMatch (8440) Type: equipmentAlarm Package: equipment.RemoteInventoryMisMatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RIMISMATCH	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Mismatch of the stored RI of FLC and BC.		
Remedial action: Mismatch of the stored Remote Inventory of the FLC and BTC		

Table 2-175 Rerouted

Alarm	Attributes	Applicable major release
Name: Rerouted (8244) Type: communicationsAlarm Package: gmpls.Rerouted Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Rerouted	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the current route of the LSP is not the nominal route.		
Remedial action: Not Available.		

Table 2-176 RerouteNotPossible

Alarm	Attributes	Applicable major release
Name: RerouteNotPossible (8243) Type: communicationsAlarm Package: gmpls.RerouteNotPossible Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RerouteNotPossible	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no backup route can be found or activated for the LSP.		
Remedial action: Not Available.		

Table 2-177 RightLanWronglyConnected

Alarm	Attributes	Applicable major release
Name: RightLanWronglyConnected (5645) Type: equipmentAlarm Package: equipment.RightLanWronglyConnected Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LANRIGHTRING	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf neighbors are missing in right LAN.		
Remedial action: Right Lan Wrongly Connected.Check the LAN Connectivity		

Table 2-178 RSVPDegraded

Alarm	Attributes	Applicable major release
Name: RSVPDegraded (8241) Type: communicationsAlarm Package: gmpls.RSVPDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RSVPDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication to the neighbor node for RSVP traffic is not working.		
Remedial action: Not Available.		

Table 2-179 RSVPDown

Alarm	Attributes	Applicable major release
Name: RSVPDown (8242) Type: communicationsAlarm Package: gmpls.RSVPDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RSVPDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the RSVP communication to the neighbor is down.		
Remedial action: Not Available.		

Table 2-180 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 2-181 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 2-182 ServerSignalFailureEth

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureEth (8085) Type: communicationsAlarm Package: optical.ServerSignalFailureEth Raised on class: optical.GigeSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSFETH	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Egress Server Signal Failure detected on Transparently Transported GBEn.		

Table 2-182 ServerSignalFailureEth (continued)

Alarm	Attributes	Applicable major release
Remedial action: Egress Server Signal Failure detected on Transparently Transported GBEn.		

Table 2-183 ServerSignalFailureOch

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureOch (8086) Type: communicationsAlarm Package: optical.ServerSignalFailureOch Raised on class: optical.OTPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSFOCH	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when server signal failure on Optical Channel detected.		
Remedial action: Server signal failure detected.		

Table 2-184 ServerSignalFailureOnLine

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureOnLine (8087) Type: communicationsAlarm Package: optical.ServerSignalFailureOnLine Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSFL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure detected.		
Remedial action: Server Signal Failure on line.		

Table 2-185 ServerSignalFailureOnPath

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureOnPath (8088) Type: communicationsAlarm Package: optical.ServerSignalFailureOnPath Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSFP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure detected.		
Remedial action: Server Signal Failure on path.		

Table 2-186 ServerSignalFailureOnSection

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureOnSection (8089) Type: communicationsAlarm Package: optical.ServerSignalFailureOnSection Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSFS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure detected.		
Remedial action: Server Signal Failure on section.		

Table 2-187 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 2-188 Servicing

Alarm	Attributes	Applicable major release
Name: Servicing (5648) Type: equipmentAlarm Package: equipment.Servicing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SERVICING	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FLC is temporarily in Servicing State.		
Remedial action: Indicates that FLC is temporarily in Servicing State.		

Table 2-189 ShelfMixedOperationMode

Alarm	Attributes	Applicable major release
Name: ShelfMixedOperationMode (5649) Type: equipmentAlarm Package: equipment.ShelfMixedOperationMode Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MIXOPERAT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf Operates in Mixed Operation Mode.		
Remedial action: Shelf operates in mixed operation mode.		

Table 2-190 ShelfOutage

Alarm	Attributes	Applicable major release
Name: ShelfOutage (5650) Type: equipmentAlarm Package: equipment.ShelfOutage Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SHTRANSMFAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when complete Outage of Shelf.		
Remedial action: Complete Outage of Shelf Transmission Functionality. Replace the Shelf		

Table 2-191 ShelfUnAvailable

Alarm	Attributes	Applicable major release
Name: ShelfUnAvailable (5651) Type: equipmentAlarm Package: equipment.ShelfUnAvailable Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SHELFUNAVAIL	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf cannot be provisioned or supervised.		
Remedial action: The Shelf equipment cannot be provisioned or supervised at the moment.		

Table 2-192 ShelfUpgradeForMtx

Alarm	Attributes	Applicable major release
Name: ShelfUpgradeForMtx (5652) Type: equipmentAlarm Package: equipment.ShelfUpgradeForMtx Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UPGSWITCH	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf ready for Matrix Size Upgrade.		
Remedial action: Shelf ready for MTX size upgrade.		

Table 2-193 ShutdownTemperatureDetected

Alarm	Attributes	Applicable major release
Name: ShutdownTemperatureDetected (5653) Type: environmentalAlarm Package: equipment.ShutdownTemperatureDetected Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: THERMSHUTD	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the temperature exceeded the shutdown threshold.		
Remedial action: The temperature of components has exceeded the shutdown threshold.		

Table 2-194 SignalDegradeBitErrorRatio

Alarm	Attributes	Applicable major release
Name: SignalDegradeBitErrorRatio (8090) Type: communicationsAlarm Package: optical.SignalDegradeBitErrorRatio Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SDBER	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bit Error Rate is greater than or equal to provisioned threshold.		
Remedial action: Bit Error Rate is greater than or equal to provisioned threshold.		

Table 2-195 SignalDegradeBitErrorRatioOnPath

Alarm	Attributes	Applicable major release
Name: SignalDegradeBitErrorRatioOnPath (8119) Type: communicationsAlarm Package: oth.SignalDegradeBitErrorRatioOnPath Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SDBERP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bit Error Rate is greater than or equal to provisioned threshold.		
Remedial action: Bit Error Rate is greater than or equal to provisioned threshold.		

Table 2-196 SignalDegradeBitErrorRatioOnSection

Alarm	Attributes	Applicable major release
Name: SignalDegradeBitErrorRatioOnSection (8120) Type: communicationsAlarm Package: oth.SignalDegradeBitErrorRatioOnSection Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SDBERS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bit Error Rate is greater than or equal to provisioned threshold.		
Remedial action: Bit Error Rate is greater than or equal to provisioned threshold.		

Table 2-197 SlippingTimeSignal

Alarm	Attributes	Applicable major release
Name: SlippingTimeSignal (8091) Type: equipmentAlarm Package: optical.SlippingTimeSignal Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLTMSIG	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is raised the timing reference frequency has moved off the required accuracy limits.		
Remedial action: Informational - the timing reference frequency has moved off the required accuracy limits. Please contact your Nokia support representative for assistance.		

Table 2-198 SNCInAutomaticRestorationDisabledMode

Alarm	Attributes	Applicable major release
Name: SNCInAutomaticRestorationDisabledMode (8245) Type: communicationsAlarm Package: gmpls. SNCInAutomaticRestorationDisabledMode Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SNCInAutomaticRestora-tionDisabledMode	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when automatic restoration is disabled for this LSP.		
Remedial action: Not Available.		

Table 2-199 SNCPDegraded

Alarm	Attributes	Applicable major release
Name: SNCPDegraded (8246) Type: communicationsAlarm Package: gmpls.SNCPDegraded Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SNCPDegraded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the LSP is not 1+1 path protected.		
Remedial action: Not Available.		

Table 2-200 SoftRerouteInProgress

Alarm	Attributes	Applicable major release
Name: SoftRerouteInProgress (8248) Type: communicationsAlarm Package: gmpls.SoftRerouteInProgress Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SoftRerouteInProgress	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a soft-reroute for a tunnel LSP is active; it represents a maintenance state of the LSP.		
Remedial action: Not Available.		

Table 2-201 SoftwareDownLoadInProgress

Alarm	Attributes	Applicable major release
Name: SoftwareDownLoadInProgress (5654) Type: equipmentAlarm Package: equipment.SoftwareDownLoadInProgress Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SWDWN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when module is being downloaded with a sw.		
Remedial action: Indicate that the identified module is being download with a Software.		

Table 2-202 SoftwareVersionMismatch

Alarm	Attributes	Applicable major release
Name: SoftwareVersionMismatch (2092) Type: communicationsAlarm Package: equipment.SoftwareVersionMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfMismatch Applicable probable causes: • SfMismatch • SWMISM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Software version mismatch is detected.		
Remedial action: This alarm is raised under the following conditions:\n a. The software on the alarmed card does not match the software on the nearest EC card because the card failed to update successfully.\n b. When all cards are not running the same software release. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Find the software version number and release number on the EC card. Compare the corresponding number in the alarmed card. If it is not the same, download the software from EC to the alarmed card.\n 2. Contact your Nokia support representative.		

Table 2-203 SRGViolation

Alarm	Attributes	Applicable major release
Name: SRGViolation (8247) Type: communicationsAlarm Package: gmpls.SRGViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SRGViolation	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when both legs (SNCP) of the LSP or the LSP to its diverse LSP are not SRG diverse. Also after a cut scenario if a new backup could not be SRG diverse (only link diverse) to the failure, the violation is raised.		
Remedial action: Not Available.		

Table 2-204 StandbyDbc

Alarm	Attributes	Applicable major release
Name: StandbyDbc (5655) Type: equipmentAlarm Package: equipment.StandbyDbc Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: STBYDBC	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the inactive FLC is unusable.		
Remedial action: The Contents of the mass storage device on the inactive FLC is corrupted and cannot be repaired		

Table 2-205 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 2-206 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 2-206 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 2-207 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 2-208 SyncEqpt

Alarm	Attributes	Applicable major release
Name: SyncEqpt (4565) Type: equipmentAlarm Package: equipment.SyncEqpt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncEqpt	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Synchronization equipment failure is detected.		
Remedial action: Refer Procedure : Clear Synchronization Equipment (CRU) failure alarm in 1830 Troubleshooting guide.		

Table 2-209 SyncOos

Alarm	Attributes	Applicable major release
Name: SyncOos (3919) Type: equipmentAlarm Package: equipment.SyncOos Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncOos	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when All selectable timing reference fail is detected.		
Remedial action: SYNCOOS (Timing reference failed (Not Protected or Protection not Available)) / SYNCOOS (Timing reference failed--system going into holdover).Check the timing reference quality and priority.Also, Check the reference status.		

Table 2-210 SyncRefFail

Alarm	Attributes	Applicable major release
Name: SyncRefFail (3736) Type: equipmentAlarm Package: optical.SyncRefFail Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncRefFail	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when timing reference fails. .		
Remedial action: Check the timing reference quality and priority.		

Table 2-211 SystemInitialization

Alarm	Attributes	Applicable major release
Name: SystemInitialization (8070) Type: equipmentAlarm Package: netw.SystemInitialization Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INIT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised to indicate that system initialization is currently in progress.		
Remedial action: System initialization is currently in progress.		

Table 2-212 SystemInitializationNewFailure

Alarm	Attributes	Applicable major release
Name: SystemInitializationNewFailure (8071) Type: equipmentAlarm Package: netw.SystemInitializationNewFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INITNF	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when system initialization failed during ISU.		
Remedial action: System initialization failed during ISU.		

Table 2-213 TBbeOdu

Alarm	Attributes	Applicable major release
Name: TBbeOdu (8121) Type: qualityOfServiceAlarm Package: oth.TBbeOdu Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Background Block Errors on ODU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-214 TBbeOdu15Min

Alarm	Attributes	Applicable major release
Name: TBbeOdu15Min (3398) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-215 TBbeOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TBbeOdu15MinOut (8446) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_15MIN_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-216 TBbeOdu1Day

Alarm	Attributes	Applicable major release
Name: TBbeOdu1Day (3399) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-217 TBbeOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TBbeOdu1DayOut (8447) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_1DAY_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-218 TBbeOtu

Alarm	Attributes	Applicable major release
Name: TBbeOtu (8122) Type: qualityOfServiceAlarm Package: oth.TBbeOtu Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_OTU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Background Block Errors on OTU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-219 TBbeOtu15Min

Alarm	Attributes	Applicable major release
Name: TBbeOtu15Min (3400) Type: qualityOfServiceAlarm Package: equipment.TBbeOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_OTU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-220 TBbeOtu1Day

Alarm	Attributes	Applicable major release
Name: TBbeOtu1Day (3401) Type: qualityOfServiceAlarm Package: equipment.TBbeOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_OTU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-221 TBbeRs15Min

Alarm	Attributes	Applicable major release
Name: TBbeRs15Min (3406) Type: qualityOfServiceAlarm Package: equipment.TBbeRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RS_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-222 TBbeRs1Day

Alarm	Attributes	Applicable major release
Name: TBbeRs1Day (3407) Type: qualityOfServiceAlarm Package: equipment.TBbeRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RS_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-223 TCvs

Alarm	Attributes	Applicable major release
Name: TCvs (8092) Type: qualityOfServiceAlarm Package: optical.TCvs Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CVS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Code Violations on Section is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-224 TerminalLoopbackConfigured (oth)

Alarm	Attributes	Applicable major release
Name: TerminalLoopbackConfigured (8381) Type: communicationsAlarm Package: oth.TerminalLoopbackConfigured Raised on class: oth.Otuk	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TerminalLoopbackConfigured	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Terminal Loopback is configured on Facility.		
Remedial action: To clear the condition, disable Terminal Loopback configured on OTUk.		

Table 2-225 TEsOdu

Alarm	Attributes	Applicable major release
Name: TEsOdu (8123) Type: qualityOfServiceAlarm Package: oth.TEsOdu Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Error Seconds on ODU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-226 TEsOdu15Min

Alarm	Attributes	Applicable major release
Name: TEsOdu15Min (3430) Type: qualityOfServiceAlarm Package: equipment.TEsOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-227 TEsOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TEsOdu15MinOut (8448) Type: qualityOfServiceAlarm Package: equipment.TEsOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_15MIN_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-228 TEsOdu1Day

Alarm	Attributes	Applicable major release
Name: TEsOdu1Day (3431) Type: qualityOfServiceAlarm Package: equipment.TEsOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-229 TEsOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TEsOdu1DayOut (8449) Type: qualityOfServiceAlarm Package: equipment.TEsOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_1DAY_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-230 TEsOtu

Alarm	Attributes	Applicable major release
Name: TEsOtu (8124) Type: qualityOfServiceAlarm Package: oth.TEsOtu Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_OTU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Error Seconds on OTU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-231 TEsOtu15Min

Alarm	Attributes	Applicable major release
Name: TEsOtu15Min (3432) Type: qualityOfServiceAlarm Package: equipment.TEsOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_OTU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-232 TEsOtu1Day

Alarm	Attributes	Applicable major release
Name: TEsOtu1Day (3433) Type: qualityOfServiceAlarm Package: equipment.TEsOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_OTU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-233 TEsRs15Min

Alarm	Attributes	Applicable major release
Name: TEsRs15Min (3442) Type: qualityOfServiceAlarm Package: equipment.TEsRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RS_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-234 TEsRs1Day

Alarm	Attributes	Applicable major release
Name: TEsRs1Day (3443) Type: qualityOfServiceAlarm Package: equipment.TEsRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RS_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-235 TEss

Alarm	Attributes	Applicable major release
Name: TEss (8093) Type: qualityOfServiceAlarm Package: optical.TEss Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ESS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Errored Seconds on Section is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-236 TestModeEnabled

Alarm	Attributes	Applicable major release
Name: TestModeEnabled (8249) Type: communicationsAlarm Package: gmpls.TestModeEnabled Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TestModeEnabled	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the LSP is in test mode and 'frozen' to its current route.		
Remedial action: Not Available.		

Table 2-237 TFecc

Alarm	Attributes	Applicable major release
Name: TFecc (8125) Type: qualityOfServiceAlarm Package: oth.TFecc Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FECC	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of FEC Errors Corrected on OTU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-238 TFecc15Min

Alarm	Attributes	Applicable major release
Name: TFecc15Min (3480) Type: qualityOfServiceAlarm Package: equipment.TFecc15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FECC_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-239 TFecc1Day

Alarm	Attributes	Applicable major release
Name: TFecc1Day (3481) Type: qualityOfServiceAlarm Package: equipment.TFecc1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FECC_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-240 TOfsRs15Min

Alarm	Attributes	Applicable major release
Name: TOfsRs15Min (5657) Type: qualityOfServiceAlarm Package: equipment.TOfsRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OFS_RS_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OFS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-241 TOfsRs1Day

Alarm	Attributes	Applicable major release
Name: TOfsRs1Day (5658) Type: qualityOfServiceAlarm Package: equipment.TOfsRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OFS_RS_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OFS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-242 TOprh

Alarm	Attributes	Applicable major release
Name: TOprh (8094) Type: qualityOfServiceAlarm Package: optical.TOprh Raised on class: optical.OTPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPR_H	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Optical Power Received (High) is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-243 TOprh15Min

Alarm	Attributes	Applicable major release
Name: TOprh15Min (3484) Type: qualityOfServiceAlarm Package: equipment.TOprh15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRH_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-244 TOprh1Day

Alarm	Attributes	Applicable major release
Name: TOprh1Day (3485) Type: qualityOfServiceAlarm Package: equipment.TOprh1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRH_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-245 TOprl

Alarm	Attributes	Applicable major release
Name: TOprl (8095) Type: qualityOfServiceAlarm Package: optical.TOprl Raised on class: optical.OTPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPR_L	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Optical Power Received (Low) is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-246 TOprl15Min

Alarm	Attributes	Applicable major release
Name: TOprl15Min (3486) Type: qualityOfServiceAlarm Package: equipment.TOprl15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRL_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-247 TOprl1Day

Alarm	Attributes	Applicable major release
Name: TOprl1Day (3487) Type: qualityOfServiceAlarm Package: equipment.TOprl1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRL_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-248 TOpth

Alarm	Attributes	Applicable major release
Name: TOpth (8096) Type: qualityOfServiceAlarm Package: optical.TOpth Raised on class: optical.OTPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPT_H	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Optical Power Transmitted (High) is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-249 TOpth15Min

Alarm	Attributes	Applicable major release
Name: TOpth15Min (3488) Type: qualityOfServiceAlarm Package: equipment.TOpth15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTH_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-250 TOpth1Day

Alarm	Attributes	Applicable major release
Name: TOpth1Day (3489) Type: qualityOfServiceAlarm Package: equipment.TOpth1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTH_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-251 TOptl

Alarm	Attributes	Applicable major release
Name: TOptl (8097) Type: qualityOfServiceAlarm Package: optical.TOptl Raised on class: optical.OTPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPT_L	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Optical Power Transmitted (Low) is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-252 TOptl15Min

Alarm	Attributes	Applicable major release
Name: TOptl15Min (3490) Type: qualityOfServiceAlarm Package: equipment.TOptl15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTL_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-253 TOptl1Day

Alarm	Attributes	Applicable major release
Name: TOptl1Day (3491) Type: qualityOfServiceAlarm Package: equipment.TOptl1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTL_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-254 TrailTraceIdentifierMismatchOnPath

Alarm	Attributes	Applicable major release
Name: TrailTraceIdentifierMismatchOnPath (8102) Type: communicationsAlarm Package: optical.TrailTraceIdentifierMismatchOnPath Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TIMP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trail Trace Identifier Mismatch on Path detected.		
Remedial action: Trail Trace Identifier Mismatch on path detected.		

Table 2-255 TrailTraceIdentifierMismatchOnSection

Alarm	Attributes	Applicable major release
Name: TrailTraceIdentifierMismatchOnSection (8103) Type: communicationsAlarm Package: optical. TrailTraceIdentifierMismatchOnSection Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TIMS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trail Trace Identifier Mismatch on Section detected.		
Remedial action: Trail Trace Identifier Mismatch on section detected.		

Table 2-256 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 2-257 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 2-258 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		

Table 2-258 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 2-259 TSefss

Alarm	Attributes	Applicable major release
Name: TSefss (8098) Type: qualityOfServiceAlarm Package: optical.TSefss Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFSS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Severely Errored Frame Seconds on Section is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-260 TSesOdu

Alarm	Attributes	Applicable major release
Name: TSesOdu (8126) Type: qualityOfServiceAlarm Package: oth.TSesOdu Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Severely Errored Seconds on ODU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-261 TSesOdu15Min

Alarm	Attributes	Applicable major release
Name: TSesOdu15Min (3512) Type: qualityOfServiceAlarm Package: equipment.TSesOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-262 TSesOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TSesOdu15MinOut (8458) Type: qualityOfServiceAlarm Package: equipment.TSesOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_15MIN_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-263 TSesOdu1Day

Alarm	Attributes	Applicable major release
Name: TSesOdu1Day (3513) Type: qualityOfServiceAlarm Package: equipment.TSesOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-264 TSesOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TSesOdu1DayOut (8459) Type: qualityOfServiceAlarm Package: equipment.TSesOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_1DAY_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-265 TSesOtu

Alarm	Attributes	Applicable major release
Name: TSesOtu (8127) Type: qualityOfServiceAlarm Package: oth.TSesOtu Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_OTU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Severely Errored Seconds on OTU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-266 TSesOtu15Min

Alarm	Attributes	Applicable major release
Name: TSesOtu15Min (3514) Type: qualityOfServiceAlarm Package: equipment.TSesOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_OTU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-267 TSesOtu1Day

Alarm	Attributes	Applicable major release
Name: TSesOtu1Day (3515) Type: qualityOfServiceAlarm Package: equipment.TSesOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_OTU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-268 TSesRs15Min

Alarm	Attributes	Applicable major release
Name: TSesRs15Min (3524) Type: qualityOfServiceAlarm Package: equipment.TSesRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RS_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-269 TSesRs1Day

Alarm	Attributes	Applicable major release
Name: TSesRs1Day (3525) Type: qualityOfServiceAlarm Package: equipment.TSesRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RS_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-270 TSess

Alarm	Attributes	Applicable major release
Name: TSess (8099) Type: qualityOfServiceAlarm Package: optical.TSess Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SESS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Severely Errored Seconds on Section is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-271 TUasOdu

Alarm	Attributes	Applicable major release
Name: TUasOdu (8128) Type: qualityOfServiceAlarm Package: oth.TUasOdu Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Unavailable Seconds on ODU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-272 TUasOdu15Min

Alarm	Attributes	Applicable major release
Name: TUasOdu15Min (3534) Type: qualityOfServiceAlarm Package: equipment.TUasOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-273 TUasOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TUasOdu15MinOut (8460) Type: qualityOfServiceAlarm Package: equipment.TUasOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_15MIN_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-274 TUasOdu1Day

Alarm	Attributes	Applicable major release
Name: TUasOdu1Day (3535) Type: qualityOfServiceAlarm Package: equipment.TUasOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-275 TUasOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TUasOdu1DayOut (8461) Type: qualityOfServiceAlarm Package: equipment.TUasOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_1DAY_OUT	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-276 TUasOtu

Alarm	Attributes	Applicable major release
Name: TUasOtu (8129) Type: qualityOfServiceAlarm Package: oth.TUasOtu Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_OTU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Unavailable Seconds on OTU Layer is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-277 TUasOtu15Min

Alarm	Attributes	Applicable major release
Name: TUasOtu15Min (3536) Type: qualityOfServiceAlarm Package: equipment.TUasOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_OTU_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-278 TUasOtu1Day

Alarm	Attributes	Applicable major release
Name: TUasOtu1Day (3537) Type: qualityOfServiceAlarm Package: equipment.TUasOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_OTU_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-279 TUasRs15Min

Alarm	Attributes	Applicable major release
Name: TUasRs15Min (3542) Type: qualityOfServiceAlarm Package: equipment.TUasRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RS_15MIN	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-280 TUasRs1Day

Alarm	Attributes	Applicable major release
Name: TUasRs1Day (3543) Type: qualityOfServiceAlarm Package: equipment.TUasRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RS_1DAY	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-281 TUass

Alarm	Attributes	Applicable major release
Name: TUass (8100) Type: qualityOfServiceAlarm Package: optical.TUass Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UASS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Threshold Crossing of Unavailable Seconds on Section is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 2-282 UnavailableTimeOdu

Alarm	Attributes	Applicable major release
Name: UnavailableTimeOdu (8130) Type: communicationsAlarm Package: oth.UnavailableTimeOdu Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UATODU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the unavailable time period detected.		
Remedial action: Unavailable time period ODU.		

Table 2-283 UnavailableTimeOtu

Alarm	Attributes	Applicable major release
Name: UnavailableTimeOtu (8131) Type: communicationsAlarm Package: oth.UnavailableTimeOtu Raised on class: oth.Otuk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UATOTU	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the unavailable time period detected.		
Remedial action: Unavailable time period OTU.		

Table 2-284 UnavailableTimeRegeneratorSection

Alarm	Attributes	Applicable major release
Name: UnavailableTimeRegeneratorSection (8106) Type: communicationsAlarm Package: optical.UnavailableTimeRegeneratorSection Raised on class: optical.OCStmSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UATRS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the unavailable time period detected.		
Remedial action: Unavailable time period detected.		

Table 2-285 UnderlyingResourceUnavailableOnPath

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceUnavailableOnPath (8132) Type: communicationsAlarm Package: oth.UnderlyingResourceUnavailableOnPath Raised on class: oth.Oduk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: URUP	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when underlying resource is unavailable on path.		
Remedial action: Underlying resource is unavailable on path.		

Table 2-286 UnderlyingResourceUnavailableOnSection

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceUnavailableOnSection (8107) Type: communicationsAlarm Package: optical. UnderlyingResourceUnavailableOnSection Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: URUS	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when underlying resource is unavailable on section.		
Remedial action: Underlying resource is unavailable on optical section.		

Table 2-287 UnderlyingResourceUnavailableOptical

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceUnavailableOptical (8108) Type: communicationsAlarm Package: optical. UnderlyingResourceUnavailableOptical Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: URUO	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when underlying resource is unavailable on optical section.		
Remedial action: Underlying resource is unavailable on optical section.		

Table 2-288 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 2-289 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 2-290 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		

Table 2-290 UpgradedBuildVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 2-291 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 2-292 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 2-293 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 2-294 UserPayloadMismatchOut

Alarm	Attributes	Applicable major release
Name: UserPayloadMismatchOut (5507) Type: communicationsAlarm Package: equipment.UserPayloadMismatchOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpUpm Applicable probable causes: • GfpUpm • GFPUPM	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing GFP User Payload Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-295 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		

Table 2-295 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 2-296 WaitToRestore

Alarm	Attributes	Applicable major release
Name: WaitToRestore (8109) Type: communicationsAlarm Package: optical.WaitToRestore Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WTR	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: (Automatic) Set on Working path of a SNCP when switching is revertive and defects have cleared on Working and the Wait to Restore timer is in effect.		
Remedial action: Wait to restore.		

Table 2-297 WaveKeyInsertionFailure

Alarm	Attributes	Applicable major release
Name: WaveKeyInsertionFailure (4609) Type: communicationsAlarm Package: equipment.WaveKeyInsertionFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mod	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card degrade - wavelength tracker channel id insertion is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 2-298 WavelengthTrackerEncodeDegrade

Alarm	Attributes	Applicable major release
Name: WavelengthTrackerEncodeDegrade (2121) Type: equipmentAlarm Package: equipment. WavelengthTrackerEncodeDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MtcesurvDgr	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port Degrade - wavelength tracker encode degrade is detected.		

Table 2-298 WavelengthTrackerEncodeDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer section MTCESURVDGR (Port degrade - wavelength tracker encode degrade) in 1830 Troubleshooting guide.		

Table 2-299 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 2-300 WTR

Alarm	Attributes	Applicable major release
Name: WTR (3927) Type: equipmentAlarm Package: optical.WTR Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Wtr	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: Switching applications - Set on working path of an SNCP when switching is revertive and effects have cleared on the working path and the Wait-to-Restore timer is in effect. \nPhotonic applications - The OT port has detected WTR at the LINEREF layer. A LINEREF detects WTR when on a timing reference and defects have cleared and the Wait to Restore timer is in effect. .		
Remedial action: Check the reference status.		

3 1830 PSS (PSS-4, PSS-8, 16/32)

3.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 3-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 3-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 3-3 ActiveFailedAPEFailed

Alarm	Attributes	Applicable major release
Name: ActiveFailedAPEFailed (9627) Type: communicationsAlarm Package: gmpls.ActiveFailedAPEFailed Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedAPEFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APE failed as POF (point of failure).		
Remedial action: Not Available.		

Table 3-4 ActiveFailedCrossConnectionProblem

Alarm	Attributes	Applicable major release
Name: ActiveFailedCrossConnectionProblem (8213) Type: communicationsAlarm Package: gmpls.ActiveFailedCrossConnectionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedCrossConnection-Problem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has failed due to a cross-connection problem. As a result, the system tries to establish a backup path in order to reroute the traffic.		
Remedial action: Not Available.		

Table 3-5 ActiveFailedEndpointFailure

Alarm	Attributes	Applicable major release
Name: ActiveFailedEndpointFailure (8214) Type: communicationsAlarm Package: gmpls.ActiveFailedEndpointFailure Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedEndpointFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when LSP drop port(s) at A-End and/or Z-End has a transmission alarm.		
Remedial action: Not Available.		

Table 3-6 ActiveFailedPreemption

Alarm	Attributes	Applicable major release
Name: ActiveFailedPreemption (8215) Type: communicationsAlarm Package: gmpls.ActiveFailedPreemption Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedPreemption	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has been preempted by another control plane service with a higher priority. As a result, the system tries to establish a backup path for the preempted service.		
Remedial action: Not Available.		

Table 3-7 ActiveFailedTransmissionProblem

Alarm	Attributes	Applicable major release
Name: ActiveFailedTransmissionProblem (8216) Type: communicationsAlarm Package: gmpls.ActiveFailedTransmissionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedTransmission-Problem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of a control plane service (with a protection type of SBR, GR, or PRC) has failed due to a transmission problem. As a result, the system tries to establish a backup path in order to reroute the traffic.		
Remedial action: Not Available.		

Table 3-8 ActiveFailedUnprotected

Alarm	Attributes	Applicable major release
Name: ActiveFailedUnprotected (8217) Type: communicationsAlarm Package: gmpls.ActiveFailedUnprotected Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveFailedUnprotected	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised an unprotected LSP has failed.		
Remedial action: Not Available.		

Table 3-9 AddPowerControlFailure

Alarm	Attributes	Applicable major release
Name: AddPowerControlFailure (4422) Type: equipmentAlarm Package: equipment.AddPowerControlFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mtcssurv Applicable probable causes: • Mtcssurv • MTCESURV	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Add power control failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-10 AesFipsFailure

Alarm	Attributes	Applicable major release
Name: AesFipsFailure (5437) Type: communicationsAlarm Package: equipment.AesFipsFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AesFipsFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AES FIPS Failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-11 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		

Table 3-11 AggregatedVFLPortDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 3-12 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 3-13 AlarmReportingControlInhibited

Alarm	Attributes	Applicable major release
Name: AlarmReportingControlInhibited (4852) Type: communicationsAlarm Package: netw.AlarmReportingControlInhibited Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ArcIND	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Alarm reporting control in indefinite inhibition mode is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-14 AlienEgrLOS

Alarm	Attributes	Applicable major release
Name: AlienEgrLOS (3954) Type: communicationsAlarm Package: equipment.AlienEgrLOS Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AlienEgrLOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Alien EGR Los is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-15 AmpDisabled

Alarm	Attributes	Applicable major release
Name: AmpDisabled (4423) Type: equipmentAlarm Package: equipment.AmpDisabled Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmpDisabled	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier disabled is detected.		
Remedial action: 1. Determine if there are any temperature alarms on the shelf. If so, check the airflow of the shelf, filler card presence, and ambient air temperature. Resolve any air flow obstructions or air-conditioner issues. 2. Perform a warm reset of the card.3. Perform a cold reset of the card.4. Reset the card.5. Replace the card.Follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 3-16 AmpDisabledC

Alarm	Attributes	Applicable major release
Name: AmpDisabledC (11071) Type: equipmentAlarm Package: equipment.AmpDisabledC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmpDisabledC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier disabled C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-17 AmpDisabledL

Alarm	Attributes	Applicable major release
Name: AmpDisabledL (11072) Type: equipmentAlarm Package: equipment.AmpDisabledL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmpDisabledL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier disabled L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-18 AmpDisabledOpticalPowerOverload

Alarm	Attributes	Applicable major release
Name: AmpDisabledOpticalPowerOverload (1970) Type: equipmentAlarm Package: equipment. AmpDisabledOpticalPowerOverload Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Ovrld	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier disabled - optical power overload is detected.		
Remedial action: 1. Determine if there are any temperature alarms on the shelf. If so, check the airflow of the shelf, filler card presence, and ambient air temperature. Resolve any air flow obstructions or air-conditioner issues. 2. Perform a warm reset of the card.3. Perform a cold reset of the card.4. Reset the card.5. Replace the card.Follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 3-19 AmpGainTooHigh

Alarm	Attributes	Applicable major release
Name: AmpGainTooHigh (4424) Type: equipmentAlarm Package: equipment.AmpGainTooHigh Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighGain	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amplifier gain too high is detected.		
Remedial action: This is a transitory alarm that is raised for a maximum of 30 seconds while the amplifier attempts to limit the output power. If after 30 seconds the output power cannot be limited,a Card Failure - Device alarm is raised.		

Table 3-20 AmpGainTooHighC

Alarm	Attributes	Applicable major release
Name: AmpGainTooHighC (11073) Type: equipmentAlarm Package: equipment.AmpGainTooHighC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighGainC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amp gain too high C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-21 AmpGainTooHighL

Alarm	Attributes	Applicable major release
Name: AmpGainTooHighL (11074) Type: equipmentAlarm Package: equipment.AmpGainTooHighL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighGainL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amp gain too high L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-22 AmpGainTooLow

Alarm	Attributes	Applicable major release
Name: AmpGainTooLow (4425) Type: equipmentAlarm Package: equipment.AmpGainTooLow Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoGain	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amplifier gain too low is detected.		
Remedial action: Please refer section LOGAIN (Amplifier out of operational range - amplifier gain too low) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-23 AmpGainTooLowC

Alarm	Attributes	Applicable major release
Name: AmpGainTooLowC (11075) Type: equipmentAlarm Package: equipment.AmpGainTooLowC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoGainC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amp gain too low C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-24 AmpGainTooLowL

Alarm	Attributes	Applicable major release
Name: AmpGainTooLowL (11076) Type: equipmentAlarm Package: equipment.AmpGainTooLowL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoGainL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier out of operational range - amp gain too low L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-25 AmpOutputPowerUnachievable

Alarm	Attributes	Applicable major release
Name: AmpOutputPowerUnachievable (1976) Type: communicationsAlarm Package: equipment.AmpOutputPowerUnachievable Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprUnachieve	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OPR unachievable is detected.		
Remedial action: Please refer section OPRUNACHIEVE (Channel Power Unachievable) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-26 AnnounceLoss

Alarm	Attributes	Applicable major release
Name: AnnounceLoss (4951) Type: communicationsAlarm Package: ptp.AnnounceLoss Raised on class: ptp.IEEEPTPPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AnnounceLoss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Announce messages on the slave port .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-27 APEInProgress

Alarm	Attributes	Applicable major release
Name: APEInProgress (9626) Type: communicationsAlarm Package: gmpls.APEInProgress Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APEInProgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when power adjustment is in progress.		
Remedial action: Not Available.		

Table 3-28 ApeInProgress

Alarm	Attributes	Applicable major release
Name: ApeInProgress (5559) Type: communicationsAlarm Package: netw.ApeInProgress Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ApeInProgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APE in progress.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-29 APRFORCED

Alarm	Attributes	Applicable major release
Name: APRFORCED (8155) Type: communicationsAlarm Package: equipment.APRFORCED Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRFORCED	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Forced.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-30 AprInvalidTopo

Alarm	Attributes	Applicable major release
Name: AprInvalidTopo (3332) Type: communicationsAlarm Package: equipment.AprInvalidTopo Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRINVALIDTOPO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Active - Invalid Topology is detected.		
Remedial action: Proceed as follows to clear the APR Active - Invalid Topology alarm.1 Create a new topology.CLI config interface topology.From WEBUI use command - Select Connections > Physical Topology > Create.		

Table 3-31 APRLIMITED

Alarm	Attributes	Applicable major release
Name: APRLIMITED (8156) Type: communicationsAlarm Package: equipment.APRLIMITED Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRLIMITED	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Limited.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-32 AprLine

Alarm	Attributes	Applicable major release
Name: AprLine (4426) Type: communicationsAlarm Package: equipment.AprLine Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRLINE	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Active - Line is detected.		
Remedial action: Determine the ingress amplifier that is connected to the egress amplifier reporting the APR condition.Check whether an APROSC condition is active on the egress amplifier at either end of the span.If so proceed to APROSC to clear the APROSC condition.Confirm the LOS condition on the ingress amplifier.Check in LOS to clear the LOS condition.The APRLINE condition will automatically clear up to 100 seconds after the ingress LOS condition has been cleared.		

Table 3-33 AprNode

Alarm	Attributes	Applicable major release
Name: AprNode (3333) Type: communicationsAlarm Package: equipment.AprNode Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRNODE	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Active - Node is detected.		
Remedial action: If no services are provisioned at the input to the LD pack, provision at least one service.If services are provisioned at the input to the LD pack, Check to LOS to clear the LOS condition.		

Table 3-34 AprOsc

Alarm	Attributes	Applicable major release
Name: AprOsc (3334) Type: communicationsAlarm Package: equipment.AprOsc Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APROSC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Active - OSC disabled is detected.		
Remedial action: Check the OSC provisioning at both ends of the span by looking at the connected ingress LD, and also at the ingress LD at the far end of the span.Set both OSCs to OC3. The condition will automatically clear within 100 seconds.		

Table 3-35 AprSwitch

Alarm	Attributes	Applicable major release
Name: AprSwitch (3335) Type: communicationsAlarm Package: equipment.AprSwitch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRSWITCH	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Active - Port Switch is detected.		
Remedial action: Some EDFA and Raman amplifier circuit packs that are capable of producing high output power, exceeding class 1M limits, are equipped with port switches on the high-power ports. Before a fiber jumper can be disconnected from the high-power port, a cover must be removed from the faceplate. A switch within the pack detects the cover removal and shuts off the amplifier within the circuit pack. After the cover is reinstalled on the circuit pack, the amplifier will restart and the alarm will clear automatically.		

Table 3-36 AprUnavail

Alarm	Attributes	Applicable major release
Name: AprUnavail (3336) Type: communicationsAlarm Package: equipment.AprUnavail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRUNAVAIL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Unavailable - Monitor Card Booting is detected.		
Remedial action: The alarm clears automatically after the reboot has been completed. No corrective action is required.		

Table 3-37 AprUnavailOsc

Alarm	Attributes	Applicable major release
Name: AprUnavailOsc (3337) Type: communicationsAlarm Package: equipment.AprUnavailOsc Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: APRUNAVAILOSC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APR Limited - OSC SFP Failure is detected.		
Remedial action: Replace the affected SFP.		

Table 3-38 ApsChannelMismatch

Alarm	Attributes	Applicable major release
Name: ApsChannelMismatch (4427) Type: communicationsAlarm Package: equipment.ApsChannelMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ApsCm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APS channel mismatch is detected.		

Table 3-38 ApsChannelMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: Observe the protection information presented in the APSCM condition. Note the protection group information and the cards involved.Login to the near end NE and determine the NE and card that link directly to the (near-end) card reporting the APSCM alarm.1.Ensure that the near-end and far-end interfaces are in the same protection group.2. Check the direction of the protection group.3. Validate that the protection group has a valid working and protection path.For Detailed steps Please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-39 ApsFarEndProtLineFail

Alarm	Attributes	Applicable major release
Name: ApsFarEndProtLineFail (4428) Type: communicationsAlarm Package: equipment.ApsFarEndProtLineFail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FePrLf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far end protection line failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-40 ApsLockoutOfProtection

Alarm	Attributes	Applicable major release
Name: ApsLockoutOfProtection (4429) Type: communicationsAlarm Package: equipment.ApsLockoutOfProtection Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LockoutOfPr Applicable probable causes: • LockoutOfPr • LockoutOfPrVTS1 • LockoutOfPrVTS2 • LockoutOfPrVTS3 • LockoutOfPrVTS4 • LockoutOfPrVTS5 • LockoutOfPrVTS6 • LockoutOfPrVTS7 • LockoutOfPrVTS8 • LockoutOfPrVTS9 • LockoutOfPrVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Lockout of protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-41 ApsModeMismatch

Alarm	Attributes	Applicable major release
Name: ApsModeMismatch (4430) Type: communicationsAlarm Package: equipment.ApsModeMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ApsMm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APS mode mismatch is detected.		

Table 3-41 ApsModeMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: Determine the protection group for the port raising this alarm and also associated shelf/slot/port on the far end NE.Check the network plan to determine the desired directionality for the protection group.If the desired directionality for the protection group is unidirectional, change the protection mode at this port and near end to uni-directional or vice versa.For Detailed steps Please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-42 ApsProtSwitchByteFail

Alarm	Attributes	Applicable major release
Name: ApsProtSwitchByteFail (4431) Type: communicationsAlarm Package: equipment.ApsProtSwitchByteFail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ApsB	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when APS protection switching byte failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-43 ApsSwitchedToWork

Alarm	Attributes	Applicable major release
Name: ApsSwitchedToWork (1977) Type: communicationsAlarm Package: equipment.ApsSwitchedToWork Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WkSwBk	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic switch to working is detected.		
Remedial action: Please refer section WKSWBK (Automatic switch to working) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-44 ApsWorkingForceSwitchedBackToWorking

Alarm	Attributes	Applicable major release
Name: ApsWorkingForceSwitchedBackToWorking (4432) Type: communicationsAlarm Package: equipment. ApsWorkingForceSwitchedBackToWorking Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdWkSwBk Applicable probable causes: • FrcdWkSwBk • FrcdWkSwBkVTS1 • FrcdWkSwBkVTS2 • FrcdWkSwBkVTS3 • FrcdWkSwBkVTS4 • FrcdWkSwBkVTS5 • FrcdWkSwBkVTS6 • FrcdWkSwBkVTS7 • FrcdWkSwBkVTS8 • FrcdWkSwBkVTS9 • FrcdWkSwBkVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to working is detected.		

Table 3-44 ApsWorkingForceSwitchedBackToWorking (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-45 ApsWorkingForceSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingForceSwitchedToProtect (4433) Type: communicationsAlarm Package: equipment.ApsWorkingForceSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdWkSwPr Applicable probable causes: • FrcdWkSwPr • FrcdWkSwPrVTS1 • FrcdWkSwPrVTS2 • FrcdWkSwPrVTS3 • FrcdWkSwPrVTS4 • FrcdWkSwPrVTS6 • FrcdWkSwPrVTS7 • FrcdWkSwPrVTS8 • FrcdWkSwPrVTS9 • FrcdWkSwPrVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-46 ApsWorkingManualSwitchedBackToWorking

Alarm	Attributes	Applicable major release
Name: ApsWorkingManualSwitchedBackToWorking (4434) Type: communicationsAlarm Package: equipment.ApsWorkingManualSwitchedBackToWorking Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManWkSwBk Applicable probable causes: • ManWkSwBk • ManWkSwBkVTS1 • ManWkSwBkVTS2 • ManWkSwBkVTS3 • ManWkSwBkVTS4 • ManWkSwBkVTS5 • ManWkSwBkVTS6 • ManWkSwBkVTS7 • ManWkSwBkVTS8 • ManWkSwBkVTS9 • ManWkSwBkVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manual switch to working is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-47 ApsWorkingManualSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingManualSwitchedToProtect (4435) Type: communicationsAlarm Package: equipment.ApsWorkingManualSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManWkSwPr Applicable probable causes: • ManWkSwPr • ManWkSwPrVTS1 • ManWkSwPrVTS2 • ManWkSwPrVTS3 • ManWkSwPrVTS4 • ManWkSwPrVTS5 • ManWkSwPrVTS6 • ManWkSwPrVTS7 • ManWkSwPrVTS8 • ManWkSwPrVTS9 • ManWkSwPrVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-47 ApsWorkingManualSwitchedToProtect (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Manual switch to protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-48 ApsWorkingSwitchedToProtect

Alarm	Attributes	Applicable major release
Name: ApsWorkingSwitchedToProtect (4436) Type: communicationsAlarm Package: equipment.ApsWorkingSwitchedToProtect Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WkSwPr Applicable probable causes: • WkSwPr • WkSwPrVTS1 • WkSwPrVTS2 • WkSwPrVTS3 • WkSwPrVTS4 • WkSwPrVTS5 • WkSwPrVTS6 • WkSwPrVTS7 • WkSwPrVTS8 • WkSwPrVTS9 • WkSwPrVTS10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic switch to protection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-49 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 3-50 AsonTopo

Alarm	Attributes	Applicable major release
Name: AsonTopo (3709) Type: communicationsAlarm Package: equipment.AsonTopo Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AsonTopo	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Intra-nodal topology failure-operator action required is detected.		

Table 3-50 AsonTopo (continued)

Alarm	Attributes	Applicable major release
Remedial action: Steps to clear this alarms: 1. Check fibers on the through path containing the AID where the ASONTOPO alarm is raised.2. Note the AID where the ASONTOPO is raised and then using NE CLI or WebUI to clear the ASONTOPO alarm.3. If no service is present over the AID where the ASONTOPO was raised, create an unprotected LSP over the AID where the ASONTOPO was raised (must be a unprotected LSP so that control plane will not remove cross connect if another problem is encountered).4. Check for any other alarms (e.g. power adjust required) and follow their corresponding corrective action procedures.5. Wait at least 10 minutes to ensure that no other alarms are raised.6. Remove the unprotected LSP if it was created in a previous step.		

Table 3-51 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 3-52 AuAisP

Alarm	Attributes	Applicable major release
Name: AuAisP (4437) Type: communicationsAlarm Package: equipment.AuAisP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuAisP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-52 AuAisP (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when AU AIS PATH is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-53 AuLopP

Alarm	Attributes	Applicable major release
Name: AuLopP (4438) Type: communicationsAlarm Package: equipment.AuLopP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuLopP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AU LOP PATH is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-54 AutoLaserOffDueToUpstreamFault

Alarm	Attributes	Applicable major release
Name: AutoLaserOffDueToUpstreamFault (4439) Type: communicationsAlarm Package: equipment. AutoLaserOffDueToUpstreamFault Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UsAls	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Auto laser off due to upstream condition is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-55 AutoNegMismatch

Alarm	Attributes	Applicable major release
Name: AutoNegMismatch (4958) Type: communicationsAlarm Package: rmd.AutoNegMismatch Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfANM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an auto negotiation mismatch is detected. Only applicable to customer ports.		
Remedial action: Please ensure that auto negotiation is configured correctly on the RMD port		

Table 3-56 AutoSwTimRef

Alarm	Attributes	Applicable major release
Name: AutoSwTimRef (3921) Type: equipmentAlarm Package: optical.AutoSwTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AutoSwTimRef	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic switch to a timing reference is detected.		
Remedial action: Check the timing reference quality and priority.		

Table 3-57 AutoSwTimRefT4

Alarm	Attributes	Applicable major release
Name: AutoSwTimRefT4 (4881) Type: equipmentAlarm Package: optical.AutoSwTimRefT4 Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AutoSwTimRef_T4	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when T4:Automatic switch to a timing reference is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-58 AutoSyncSw

Alarm	Attributes	Applicable major release
Name: AutoSyncSw (3714) Type: equipmentAlarm Package: equipment.AutoSyncSw Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AutoSyncSw	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Automatic timing reference switch is detected.		
Remedial action: AUTOSYNCSW is an event. No clearing procedure is required.		

Table 3-59 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		

Table 3-59 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 3-60 B1SignalDegrade

Alarm	Attributes	Applicable major release
Name: B1SignalDegrade (1980) Type: communicationsAlarm Package: equipment.B1SignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: B1Sd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when B1 Signal Degrade is detected.		
Remedial action: Steps to clear this alarms:1. Retrieve power level reading on the local port.2. Clean the fiber.3. If cleaning the fiber does not clear the problem, replace the fiber.4. If the power level is within the operating range, check for pluggable module alarms.5. Replace the pluggable module.		

Table 3-61 BackplaneBatteryOff

Alarm	Attributes	Applicable major release
Name: BackplaneBatteryOff (1981) Type: equipmentAlarm Package: equipment.BackplaneBatteryOff Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Pwr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Battery power at backplane off or voltage low is detected.		
Remedial action: Please refer section PWR in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-62 BackupUnavail

Alarm	Attributes	Applicable major release
Name: BackupUnavail (5560) Type: communicationsAlarm Package: netw.BackupUnavail Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackupUnavail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when backup unavailable.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-63 BackupUnavailable

Alarm	Attributes	Applicable major release
Name: BackupUnavailable (8218) Type: communicationsAlarm Package: gmpls.BackupUnavailable Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackupUnavailable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is no inactive backup path is available. In case of failures, SBR will be used. This alarm is only relevant for LSPs with GR service type.		
Remedial action: Not Available.		

Table 3-64 BackwardDefectIndication

Alarm	Attributes	Applicable major release
Name: BackwardDefectIndication (4444) Type: communicationsAlarm Package: equipment.BackwardDefectIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Bdi Applicable probable causes: • Bdi • BdiOdu • BackwardDefectIndicationEgress • BDIS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Backward Defect Indication - OTU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-65 BackwardDefectIndicationEgress

Alarm	Attributes	Applicable major release
Name: BackwardDefectIndicationEgress (4914) Type: communicationsAlarm Package: equipment.BackwardDefectIndicationEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackwardDefectIndicationEgress Applicable probable causes: • BackwardDefectIndicationEgress • BDIP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Backward Defect Indication Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-66 BadClkFreq

Alarm	Attributes	Applicable major release
Name: BadClkFreq (5438) Type: communicationsAlarm Package: equipment.BadClkFreq Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BadClkFreq	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Clock freq error > 54.6 ppm (>20 ppm causes OTN errors) .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-67 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 3-68 BatteryOff

Alarm	Attributes	Applicable major release
Name: BatteryOff (1982) Type: equipmentAlarm Package: equipment.BatteryOff Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Pwr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Battery off or power filter off is detected.		

Table 3-68 BatteryOff (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer section PWR in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-69 BdiOduOut

Alarm	Attributes	Applicable major release
Name: BdiOduOut (4445) Type: communicationsAlarm Package: equipment.BdiOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BdiOduOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Backward Defect Indication - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-70 BdLnkSpd

Alarm	Attributes	Applicable major release
Name: BdLnkSpd (11077) Type: equipmentAlarm Package: equipment.BdLnkSpd Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BdLnkSpd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bad link speed .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-71 BITSAIS

Alarm	Attributes	Applicable major release
Name: BITSAIS (4440) Type: communicationsAlarm Package: equipment.BITSAIS Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSAIS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS is detected is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-72 BITSLof

Alarm	Attributes	Applicable major release
Name: BITSLof (4441) Type: communicationsAlarm Package: equipment.BITSLof Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSLof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-73 BITSLos

Alarm	Attributes	Applicable major release
Name: BITSLos (4442) Type: communicationsAlarm Package: equipment.BITSLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-74 BITSMAN

Alarm	Attributes	Applicable major release
Name: BITSMAN (4443) Type: communicationsAlarm Package: equipment.BITSMAN Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSMAN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Logic removal of the BITS port is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-75 BoardEqpt

Alarm	Attributes	Applicable major release
Name: BoardEqpt (3338) Type: equipmentAlarm Package: equipment.BoardEqpt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BoardEqpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - boot failure is detected.		
Remedial action: The alarm is raised when a card fails to initialize.See relevant section in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-76 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 3-77 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-77 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 3-78 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 3-79 BothTimingModulesFailed

Alarm	Attributes	Applicable major release
Name: BothTimingModulesFailed (1984) Type: equipmentAlarm Package: equipment.BothTimingModulesFailed Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncClkFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing synchronization units both failed is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-80 Breaker1BatteryFeedDown

Alarm	Attributes	Applicable major release
Name: Breaker1BatteryFeedDown (4446) Type: equipmentAlarm Package: equipment.Breaker1BatteryFeedDown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Pwr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Filter 1 off or voltage low is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-81 Breaker2BatteryFeedDown

Alarm	Attributes	Applicable major release
Name: Breaker2BatteryFeedDown (4447) Type: equipmentAlarm Package: equipment.Breaker2BatteryFeedDown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Pwr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Filter 2 off or voltage low is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-82 BreakerCardsMismatched

Alarm	Attributes	Applicable major release
Name: BreakerCardsMismatched (4448) Type: equipmentAlarm Package: equipment.BreakerCardsMismatched Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Filter Mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-83 CardBoot

Alarm	Attributes	Applicable major release
Name: CardBoot (3715) Type: equipmentAlarm Package: equipment.CardBoot Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardBoot	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card booting is detected.		
Remedial action: No corrective action is required. This alarm clears automatically once the card is booted.		

Table 3-84 CardClkOffFreq

Alarm	Attributes	Applicable major release
Name: CardClkOffFreq (5439) Type: communicationsAlarm Package: equipment.CardClkOffFreq Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardClkOffFreq	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card Clock Frequency measured out of spec .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-85 CardDegrade

Alarm	Attributes	Applicable major release
Name: CardDegrade (1987) Type: equipmentAlarm Package: equipment.CardDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card degrade - device is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Is the alarmed pack a 100G Coherent OT (112SCA1, 112SNA1, 112SCX10 or 112SNX10)? 2. Check the line port information and Line port PM.If the OPT and OPR parameters are blank go to Step 3.3. Check the firmware profile that is currently running on the pack.If not, go to Step 7.If the firmware profile for the card is lower than the versions shown in the table below,then the firmware should be upgraded see - Selecting a Specific Firmware Version 4. Perform a cold reset of the card.5. Reseat the card.6. Replace the card.7. Perform a warm reset of the card.		

Table 3-86 CardDegradeMonitorFailure

Alarm	Attributes	Applicable major release
Name: CardDegradeMonitorFailure (4451) Type: equipmentAlarm Package: equipment.CardDegradeMonitorFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgrMon	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when HW_HUDSON_FPGA failure is detected.		

Table 3-86 CardDegradeMonitorFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Refer Procedure : Clear Card Degrade - Device in 1830 Troubleshooting guide.		

Table 3-87 CardFailCru

Alarm	Attributes	Applicable major release
Name: CardFailCru (11081) Type: equipmentAlarm Package: equipment.CardFailCru Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptCru	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - clock recovery unit .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-88 CardFailure

Alarm	Attributes	Applicable major release
Name: CardFailure (1988) Type: equipmentAlarm Package: equipment.CardFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Eqpt Applicable probable causes: • Eqpt • ContEqpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - device is detected.		
Remedial action: 1. Perform a warm reset of the card.2.Perform a cold reset of the card.3. Reset the card.4. Replace the card.		

Table 3-89 CardInitBcm

Alarm	Attributes	Applicable major release
Name: CardInitBcm (4452) Type: equipmentAlarm Package: equipment.CardInitBcm Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardInitBcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card Initializing - BCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-90 CardInitializing

Alarm	Attributes	Applicable major release
Name: CardInitializing (1989) Type: equipmentAlarm Package: equipment.CardInitializing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardInit	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card initializing is detected.		
Remedial action: This condition should clear by itself, or be replaced by another card alarm. No corrective action is required.The condition clears or is replaced by a card alarm. If the alarm does not clear, then follow the procedure - Card Failure.Note: To get correct PM counts after an MSC cold reboot, initialize the PM registers.		

Table 3-91 CardInitNonBcm

Alarm	Attributes	Applicable major release
Name: CardInitNonBcm (4453) Type: equipmentAlarm Package: equipment.CardInitNonBcm Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardInitNonBcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card Initializing - NONBCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-92 CardMismatch

Alarm	Attributes	Applicable major release
Name: CardMismatch (1160) Type: equipmentAlarm Package: equipment.CardMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card mismatch is detected.		
Remedial action: 1. Display the provisioned card type.2. Verify from the network plan what type of card is supposed to be in that slot.3. If the inserted card is the incorrect type, remove the card and insert one that matches the provisioned type for the slot.If the provisioning is incorrect, then reconfigure to make the provisioning match the card.If the provisioning is correct and the card is of a matching type, then there is an issue with the card itself. Continue with Step 4.4. Perform a warm reset of the card.5.Perform a cold reset of the card.6. Reseat the card.7. Replace the card.		

Table 3-93 CardMissing

Alarm	Attributes	Applicable major release
Name: CardMissing (1990) Type: equipmentAlarm Package: equipment.CardMissing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplUnitMiss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card missing is detected.		

Table 3-93 CardMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: The process for variable 1830 PSS nodes are different to clear this alarm.Please refer 1830 Trouble Shooting guide, section - REPLUNTMISS (Card Missing) to follow detailed steps for clearing this alarm.		

Table 3-94 CardNotAllowed

Alarm	Attributes	Applicable major release
Name: CardNotAllowed (1991) Type: equipmentAlarm Package: equipment.CardNotAllowed Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardNotAllowed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card not allowed is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Identify that the Wavelength Tracker mode of the shelf is set correctly.2. If the Wavelength Tracker mode is disabled, remove the affected card.		

Table 3-95 CardPowerOff

Alarm	Attributes	Applicable major release
Name: CardPowerOff (11082) Type: equipmentAlarm Package: equipment.CardPowerOff Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CRDPWROFF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card power off .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-96 CardProvisioningFailure

Alarm	Attributes	Applicable major release
Name: CardProvisioningFailure (1992) Type: equipmentAlarm Package: equipment.CardProvisioningFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DataFlt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card provisioning failure is detected.		

Table 3-96 CardProvisioningFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Determine if there is a software mismatch on the NE. If so, resolve the software issue first. The NE should be running with a committed software load. CLI show software upgrade status alm WEBUI Select Administration > Software > Upgrade and view the Status field.2. Perform a warm reset on the card that has the DATAFLT condition raised against it.CLI config card card type shelf slot reset warm WEBUI Select the card, click the Reboot tab, select Warm Reboot >Submit.3. Perform a warm reset on the Equipment Controller. This will cause a Equipment Controller switch in a redundant configuration.4. Perform a cold reset on the alarmed card. CLI config card card type shelf slot reset cold WEBUI Select the card, click the Reboot tab, select Cold Reboot >Submit.5. Delete the services and de-provision the alarmed card. Re-provision the card with the same parameters as was previously done.6. Reseat the alarmed card.7. Replace the alarmed card.		

Table 3-97 CardSanityFailure

Alarm	Attributes	Applicable major release
Name: CardSanityFailure (1993) Type: equipmentAlarm Package: equipment.CardSanityFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardSanity	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - sanity is detected.		
Remedial action: The alarms clearing procedures are similar to Card Failure - Communication.1. Perform a warm reset of the card.2.Perform a cold reset of the card.3. Reseat the card.4. Replace the card.		

Table 3-98 CardThermShutdown

Alarm	Attributes	Applicable major release
Name: CardThermShutdown (11083) Type: equipmentAlarm Package: equipment.CardThermShutdown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ThermShutdown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - thermal shutdown .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-99 CardUnknown

Alarm	Attributes	Applicable major release
Name: CardUnknown (1994) Type: equipmentAlarm Package: equipment.CardUnknown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Unknown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card unknown is detected.		

Table 3-99 CardUnknown (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Verify if the inserted card is supported for the current running release.2. If the card is not yet supported in this release and the card is a required type for the NE, verify that the correct release is running on the NE. Upgrade the NE to the correct release if it is not to support this card type.3. If the NE is running the correct release but the card is not yet supported in that release, remove the card and replace it with one that is supported by the software running on the NE.4. If the card is supported and the NE is running the correct release, the problem may be with the card itself.5. Perform a warm reset of the card.6.Perform a cold reset of the card.7. Reseat the card.8. Replace the card.		

Table 3-100 CBandLossOfSignal

Alarm	Attributes	Applicable major release
Name: CBandLossOfSignal (4449) Type: communicationsAlarm Package: equipment.CBandLossOfSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AllChanMiss Applicable probable causes: • AllChanMiss • AllChanMissOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when All Channels Missing is detected.		
Remedial action: Follow the following steps to clear the alarm:1. List the cross-connects.2. Confirm that all cross-connects are administratively up. To bring a cross-connect Admin Up.3. Check for any channel alarms and resolve.4. Verify that the cards and ports upstream of the LDs DCM or Line In port (that is, within the NE for Egress amp, line port faces external to the NE for Ingress amp) are alarm free.Resolve any alarms on cards/ports that are upstream of the LD pack using the information gathered in Step 1.5. Verify that there is a fiber properly plugged into the LDs DCM or Line In port, that the fiber is the correct type, and that the other end of the fiber is connected properly.6. Verify that the input power to the alarmed port is within limits:If the power is too low, verify that the fiber is not damaged or dirty, and clean or replace if necessary.7. If the problem is not resolved, then replace the card.		

Table 3-101 CBandLossOfSignalC

Alarm	Attributes	Applicable major release
Name: CBandLossOfSignalC (11078) Type: communicationsAlarm Package: equipment.CBandLossOfSignalC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AllChanMissOutC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when All Outgoing Channels Missing C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-102 CBandLossOfSignalL

Alarm	Attributes	Applicable major release
Name: CBandLossOfSignalL (11079) Type: communicationsAlarm Package: equipment.CBandLossOfSignalL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AllChanMissOutL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when All Outgoing Channels Missing L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-103 CFCAPACITYWARNING

Alarm	Attributes	Applicable major release
Name: CFCAPACITYWARNING (8431) Type: equipmentAlarm Package: equipment.CFCAPACITYWARNING Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CFCAPACITYWARNING	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Compact Flash needs to be Upgraded.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-104 ChannelAssignmentViolation

Alarm	Attributes	Applicable major release
Name: ChannelAssignmentViolation (9628) Type: communicationsAlarm Package: gmpls.ChannelAssignmentViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ChannelAssignmentViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the active route of LSP uses a channel that violates the allowed wavelength set of a link.		
Remedial action: Not Available.		

Table 3-105 ChannelCollision

Alarm	Attributes	Applicable major release
Name: ChannelCollision (4454) Type: communicationsAlarm Package: equipment.ChannelCollision Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchCollision Applicable probable causes: • OchCollision • UsOchCollision • OchCollisionOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel collision is detected.		
Remedial action: This alarm is raised when Wavelength Tracker has detected more than one instance of the same channel at this port. Please follow the below steps to clear this alarm:\n 1. Perform a path power trace to identify the network path the particular alarmed channel is traversing.\n 2. Determine if there is a NE where an OCHCOLLISION-OUT condition is present.\n 3. Resolve the OCHCOLLISION-OUT condition(if present).\n 4. Perform a warm reset of the card.\n 5. Perform a cold reset of the card.\n 6. Reseat the card.\n 7. Replace the card.\n For Detailed steps Please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-106 ChannelPowerOutOfRange

Alarm	Attributes	Applicable major release
Name: ChannelPowerOutOfRange (4455) Type: communicationsAlarm Package: equipment.ChannelPowerOutOfRange Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Opr Applicable probable causes: • Opr • OprOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel optical power out of range is detected.		

Table 3-106 ChannelPowerOutOfRange (continued)

Alarm	Attributes	Applicable major release
Remedial action: Refer Procedure : Clear Channel power unstable alarm in 1830 Troubleshooting guide.		

Table 3-107 ChannelSwitchingFailure

Alarm	Attributes	Applicable major release
Name: ChannelSwitchingFailure (4456) Type: equipmentAlarm Package: equipment.ChannelSwitchingFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwMtxMod	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Switching matrix module failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-108 ChannelViolation

Alarm	Attributes	Applicable major release
Name: ChannelViolation (5561) Type: communicationsAlarm Package: netw.ChannelViolation Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ChannelViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when channel assignment violation.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-109 CKM

Alarm	Attributes	Applicable major release
Name: CKM (3955) Type: communicationsAlarm Package: equipment.CKM Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CKM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Encryption Current Key Mismatch is detected.		
Remedial action: Please refer to node Troubleshooting guide for detailed steps for corrective action.		

Table 3-110 CKWKATMismatch

Alarm	Attributes	Applicable major release
Name: CKWKATMismatch (11080) Type: communicationsAlarm Package: equipment.CKWKATMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CKWKATMis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Encryption WKAT Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-111 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		

Table 3-111 ClientDelegateServerStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 3-112 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 3-113 ColorViolation (netw)

Alarm	Attributes	Applicable major release
Name: ColorViolation (5562) Type: communicationsAlarm Package: netw.ColorViolation Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ColorViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when color violation.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-114 ColorViolation (gmpls)

Alarm	Attributes	Applicable major release
Name: ColorViolation (5562) Type: communicationsAlarm Package: gmpls.ColorViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ColorViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route of the LSP breaks the color constraints regarding the specified include or exclude colors.		
Remedial action: Not Available.		

Table 3-115 CommDeg

Alarm	Attributes	Applicable major release
Name: CommDeg (5563) Type: communicationsAlarm Package: netw.CommDeg Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CommDeg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when CPNeighbor degraded.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-116 CommDown

Alarm	Attributes	Applicable major release
Name: CommDown (5564) Type: communicationsAlarm Package: netw.CommDown Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CommDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when CPNeighbor down.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-117 ConfigMM

Alarm	Attributes	Applicable major release
Name: ConfigMM (8157) Type: equipmentAlarm Package: equipment.ConfigMM Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PacketCardConfigMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is Configuration mismatch.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-118 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 3-118 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 3-119 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 3-120 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 3-121 ContEqptSplit

Alarm	Attributes	Applicable major release
Name: ContEqptSplit (4457) Type: equipmentAlarm Package: equipment.ContEqptSplit Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ContEqptSplit	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC-MTX function running on standby MTC1T9 is detected.		

Table 3-121 ContEqptSplit (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-122 ControlCardRedundancyCompromised

Alarm	Attributes	Applicable major release
Name: ControlCardRedundancyCompromised (1998) Type: equipmentAlarm Package: equipment. ControlCardRedundancyCompromised Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwEqpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Control Card redundancy is compromised is detected.		
Remedial action: Please refer section SWEQPT (Equipment Controller redundancy is compromised) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-123 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 3-124 CPUPERFORMANCE

Alarm	Attributes	Applicable major release
Name: CPUPERFORMANCE (4450) Type: equipmentAlarm Package: equipment.CPUPERFORMANCE Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPUPERFORMANCE	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when CPU Performance Issue Detected is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-125 CSF

Alarm	Attributes	Applicable major release
Name: CSF (3956) Type: communicationsAlarm Package: equipment.CSF Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Client Signal Failure -ODU is detected.		
Remedial action: See Procedure - Clear Client Signal Fail detected on the ODU in 1830 Troubleshooting guide.		

Table 3-126 CsfGfp

Alarm	Attributes	Applicable major release
Name: CsfGfp (4915) Type: communicationsAlarm Package: equipment.CsfGfp Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CsfGfp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Client Signal Fail detected on the GFP .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-127 CsfGfpOut

Alarm	Attributes	Applicable major release
Name: CsfGfpOut (4458) Type: communicationsAlarm Package: equipment.CsfGfpOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CsfGfpOut Applicable probable causes: • CsfGfpOut • GFPCSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Client Signal Fail detected on the GFP is detected.		
Remedial action: Refer Procedure: Clear Client Signal Failure (GFP) in 1830 Troubleshooting guide.		

Table 3-128 CSFODUEGR

Alarm	Attributes	Applicable major release
Name: CSFODUEGR (3957) Type: communicationsAlarm Package: equipment.CSFODUEGR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CSFODUEGR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Egress Client Signal Failure -ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-129 CsfOduOut

Alarm	Attributes	Applicable major release
Name: CsfOduOut (4459) Type: communicationsAlarm Package: equipment.CsfOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CsfOduOut Applicable probable causes: • CsfOduOut • ODUCSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Client Signal Fail detected on the ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-130 DatabaseInvalid

Alarm	Attributes	Applicable major release
Name: DatabaseInvalid (4853) Type: communicationsAlarm Package: netw.DatabaseInvalid Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbInvalid	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Database invalid is detected.		
Remedial action: Please refer DBINVALID (Database invalid) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-131 DatabaseSyncFailure

Alarm	Attributes	Applicable major release
Name: DatabaseSyncFailure (4854) Type: communicationsAlarm Package: netw.DatabaseSyncFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbMemTrf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Database synchronization failure is detected.		
Remedial action: Please refer section DBMEMTRF (Database synchronization failure) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-132 DatabaseUnsync

Alarm	Attributes	Applicable major release
Name: DatabaseUnsync (4855) Type: communicationsAlarm Package: netw.DatabaseUnsync Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbUnsync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Active and standby Main EC databases are not synchronized is detected.		
Remedial action: This is a transitional demerit that is raised when database synchronization begins, and clears once the database has been fully synchronized from the active to the inactive Equipment Controller. Typically no user action is required, however if the condition persists, perform a warm reset on the inactive Equipment Controller.		

Table 3-133 DataErr

Alarm	Attributes	Applicable major release
Name: DataErr (4464) Type: communicationsAlarm Package: equipment.DataErr Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DataErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Data Error or Timeout is detected.		
Remedial action: Refer section Procedure: Clear Data error or timeout in 1830 Troubleshooting guide.		

Table 3-134 DbCrcTypeMis

Alarm	Attributes	Applicable major release
Name: DbCrcTypeMis (11178) Type: communicationsAlarm Package: netw.DbCrcTypeMis Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbCrcTypeMis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when DB restore fail - CRC type incorrect .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-135 DbFailureLocal

Alarm	Attributes	Applicable major release
Name: DbFailureLocal (4856) Type: communicationsAlarm Package: netw.DbFailureLocal Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbFl	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when DB Failure Local - copy creation processing failure is detected.		
Remedial action: 1.Retry the database backup.2.Contact your Nokia support representative.		

Table 3-136 DbFailureTransport

Alarm	Attributes	Applicable major release
Name: DbFailureTransport (4857) Type: communicationsAlarm Package: netw.DbFailureTransport Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbFt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when DB Failure Transport - file transport failure is detected.		
Remedial action: 1.Retry the database backup.2.Contact your Nokia support representative.		

Table 3-137 DegOut

Alarm	Attributes	Applicable major release
Name: DegOut (4465) Type: communicationsAlarm Package: equipment.DegOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DegOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Signal Degrade - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-138 DelayResLoss

Alarm	Attributes	Applicable major release
Name: DelayResLoss (4952) Type: communicationsAlarm Package: ptp.DelayResLoss Raised on class: ptp.IEEEPTPPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DelayResLoss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Delay_Resp messages on the slave port .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-139 DeviceNotReachable

Alarm	Attributes	Applicable major release
Name: DeviceNotReachable (4959) Type: equipmentAlarm Package: rmd.DeviceNotReachable Raised on class: rmd.Device	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdDNR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the RMD Device is not reachable.		
Remedial action: Informational - Please check connectivity between the NE and the RMD.		

Table 3-140 DiagnosticTerminalLoopbackActive

Alarm	Attributes	Applicable major release
Name: DiagnosticTerminalLoopbackActive (2001) Type: equipmentAlarm Package: equipment.DiagnosticTerminalLoopbackActive Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LpbkTerm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Diagnostic Terminal loopback active is detected.		
Remedial action: Remove the loopback from the port.		

Table 3-141 DiscoveredPhysicalLinkMismatch

Alarm	Attributes	Applicable major release
Name: DiscoveredPhysicalLinkMismatch (657) Type: configurationAlarm Package: netw.DiscoveredPhysicalLinkMismatch Raised on class: netw.AbstractPhysicalLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: endPointUsedByNumerousLinks	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one endpoint of a physical link is used as an endpoint in another physical link.		
Raising condition: ('physicalLinkMismatchConfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMismatchConfigured' EQUAL 'false')		

Table 3-141 DiscoveredPhysicalLinkMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. Physical link endpoint (i.e. ports) can only be configured in one link.		

Table 3-142 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 3-143 DPRDegraded

Alarm	Attributes	Applicable major release
Name: DPRDegraded (8219) Type: communicationsAlarm Package: gmpls.DPRDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the OSPF routing protocol, which is used for data plane routing (DPR) between the adjacent nodes, is not fully operational.		
Remedial action: Not Available.		

Table 3-144 DPRDown

Alarm	Attributes	Applicable major release
Name: DPRDown (8220) Type: communicationsAlarm Package: gmpls.DPRDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication to the adjacent node for OSPF data plane routing is not working.		
Remedial action: Not Available.		

Table 3-145 DPRNetworkVersionMismatch

Alarm	Attributes	Applicable major release
Name: DPRNetworkVersionMismatch (8221) Type: communicationsAlarm Package: gmpls.DPRNetworkVersionMismatch Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DPRNetworkVersionMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the GMRE active network version of the adjacent node does not match the active network version of the local node.		
Remedial action: Not Available.		

Table 3-146 DuplicatePhysicalLinks

Alarm	Attributes	Applicable major release
Name: DuplicatePhysicalLinks (658) Type: configurationAlarm Package: netw.DuplicatePhysicalLinks Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicatePhysicalLinkConfig-ured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is more then one physical link configured between two endpoints.		
Raising condition: ('duplicateLinkConfigured' EQUAL 'true')		
Clearing condition: ('duplicateLinkConfigured' EQUAL 'false')		

Table 3-146 DuplicatePhysicalLinks (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The duplicated link must be deleted.		

Table 3-147 DuplicateTrailName

Alarm	Attributes	Applicable major release
Name: DuplicateTrailName (4466) Type: communicationsAlarm Package: equipment.DuplicateTrailName Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchTrailDup	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Duplicate OCH Trail name is detected.		
Remedial action: This can happen if the loopback IP address of the sourcing NE was recently changed. In the case of a loopback IP address change, the condition resolves itself after one hour.This situation can also happen if one of the following situations occur:if the control network was segmented when the OCH trails were created. If the control network is rejoined then any duplicates are discovered and this alarm is raised. The control network is segmented if the one or more ALPHG CN links are down such that a number of NEs cannot communicate to the remainder of the NEs in the network. if a database with a duplicate Och-trail is restored on a NE.if two Och Trails with the identical name are created at the same time within the network		

Table 3-148 DuplicateWaveKey

Alarm	Attributes	Applicable major release
Name: DuplicateWaveKey (4467) Type: communicationsAlarm Package: equipment.DuplicateWaveKey Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchKeyDup	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Duplicate Wave Key is detected.		
Remedial action: The alarm lists the IP address and shelf/slot/port for the other NE sourcing the same OCHtrail name.1. Check if there are any existing communication-related alarms and troubleshoot them first.2. Choose one of the connections to be rekeyed.3. Log into the NE that sources the connection to be rekeyed.4. List the cross connects that currently exist on-NE.5. Search the list for the OCh trail in question and record the A-end, Z-end, band and channel for that connection (you will use this in Step 6).6. Rekey the associated connection.		

Table 3-149 DwAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DwAlarmIndicationSignal (2004) Type: communicationsAlarm Package: equipment.DwAlarmIndicationSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DwAis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS is detected.		

Table 3-149 DwAlarmIndicationSignal (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-150 DwLossOfFrame

Alarm	Attributes	Applicable major release
Name: DwLossOfFrame (4468) Type: communicationsAlarm Package: equipment.DwLossOfFrame Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Frame - OTU is detected.		
Remedial action: This alarm indicates that a receiver port on one of the optical cards has detected a Loss of Frame. For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-151 DwLossOfMultiFrame

Alarm	Attributes	Applicable major release
Name: DwLossOfMultiFrame (4469) Type: communicationsAlarm Package: equipment.DwLossOfMultiFrame Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DwLom	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Multiframe - OTU is detected.		
Remedial action: This alarm is raised at an OT port when the OT receiver cannot synchronize to a multiframe indicator of an incoming OTUk bit stream. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Query the receive power on the port where the LOM condition is present.\n 2. Check the immediate upstream OT for any alarm conditions. If there are any, clear the failures.\n 3.Perform a warm reset of the card.\n 4.Perform a cold reset of the card.\n 5.Reseat the OT.\n 6.Replace the OT.		

Table 3-152 DwSignalDegrade

Alarm	Attributes	Applicable major release
Name: DwSignalDegrade (4470) Type: communicationsAlarm Package: equipment.DwSignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DegOtu	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Signal Degrade - OTU is detected.		

Table 3-152 DwSignalDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that OT port has detected a Signal Degrade Bit Error Rate(SDBER) on the OC-n/STM-n port of the applicable card. Please follow the below steps to clear this alarm:\n 1. Retrieve power level reading on the local port.\n 2. Clean the fiber.\n 3. If cleaning the fiber does not clear the problem, replace the fiber.\n 4. If the power level is within the operating range, check for pluggable module alarms.\n 5. Replace the pluggable module.		

Table 3-153 DwSignalFailure

Alarm	Attributes	Applicable major release
Name: DwSignalFailure (2005) Type: communicationsAlarm Package: equipment.DwSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when BER signal fail is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-154 E1AisEgr

Alarm	Attributes	Applicable major release
Name: E1AisEgr (3339) Type: communicationsAlarm Package: equipment.E1AisEgr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1AisEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS Line/MS Egress is detected.		
Remedial action: Please see AIS Line/MS in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-155 E1AisL

Alarm	Attributes	Applicable major release
Name: E1AisL (3340) Type: communicationsAlarm Package: equipment.E1AisL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1AisL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS Line/MS is detected.		
Remedial action: Please see AIS Line/MS in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-156 E1Lof

Alarm	Attributes	Applicable major release
Name: E1Lof (3341) Type: communicationsAlarm Package: equipment.E1Lof Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1Lof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer LOF (Loss of Frame) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-157 E1LofEgr

Alarm	Attributes	Applicable major release
Name: E1LofEgr (3342) Type: communicationsAlarm Package: equipment.E1LofEgr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1LofEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Frame Egress is detected.		
Remedial action: Please refer LOFEGR (Loss of Frame Egress) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-158 E1Los

Alarm	Attributes	Applicable major release
Name: E1Los (3343) Type: communicationsAlarm Package: equipment.E1Los Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1Los	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of signal is detected.		
Remedial action: Please refer LOS (Loss of Signal) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-159 E1NoCRC4M

Alarm	Attributes	Applicable major release
Name: E1NoCRC4M (3344) Type: communicationsAlarm Package: equipment.E1NoCRC4M Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1NoCRC4M	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when No CRC4 M is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-160 E1NoCRC4MEgr

Alarm	Attributes	Applicable major release
Name: E1NoCRC4MEgr (3345) Type: communicationsAlarm Package: equipment.E1NoCRC4MEgr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1NoCRC4MEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when No CRC4 M Egress is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-161 E1Rai

Alarm	Attributes	Applicable major release
Name: E1Rai (3346) Type: communicationsAlarm Package: equipment.E1Rai Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1Rai	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when E1-RAI is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-162 E1RaiEgr

Alarm	Attributes	Applicable major release
Name: E1RaiEgr (3347) Type: communicationsAlarm Package: equipment.E1RaiEgr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: E1RaiEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when E1-RAI Egress is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-163 Ebero

Alarm	Attributes	Applicable major release
Name: Ebero (3348) Type: communicationsAlarm Package: equipment.Ebero Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EBERO Applicable probable causes: • EBERO • EBER	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical supervision channel excessive BER is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-164 EcModeMismatch

Alarm	Attributes	Applicable major release
Name: EcModeMismatch (11084) Type: equipmentAlarm Package: equipment.EcModeMismatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EcModeMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Security mode support on ECs in the same shelf mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-165 EcTypeMismatch

Alarm	Attributes	Applicable major release
Name: EcTypeMismatch (11085) Type: equipmentAlarm Package: equipment.EcTypeMismatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EcTypeMis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The type of active/standby ECs in the same shelf mismatch.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-166 EfmLossOfProtocol

Alarm	Attributes	Applicable major release
Name: EfmLossOfProtocol (4960) Type: communicationsAlarm Package: rmd.EfmLossOfProtocol Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RMDEfmLosP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an EFM Loss of Protocol is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-167 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 3-168 EgressSSF

Alarm	Attributes	Applicable major release
Name: EgressSSF (3958) Type: communicationsAlarm Package: equipment.EgressSSF Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EgressSSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Egress Server Signal Failure - Client is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-169 EncapsulationFailure

Alarm	Attributes	Applicable major release
Name: EncapsulationFailure (2007) Type: communicationsAlarm Package: equipment.EncapsulationFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FecFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Encapsulation FEC mode failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-170 EnvInput1Active

Alarm	Attributes	Applicable major release
Name: EnvInput1Active (4471) Type: environmentalAlarm Package: equipment.EnvInput1Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput1Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 1 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-171 EnvInput2Active

Alarm	Attributes	Applicable major release
Name: EnvInput2Active (4472) Type: environmentalAlarm Package: equipment.EnvInput2Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput2Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 2 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-172 EnvInput3Active

Alarm	Attributes	Applicable major release
Name: EnvInput3Active (4473) Type: environmentalAlarm Package: equipment.EnvInput3Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput3Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 3 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-173 EnvInput4Active

Alarm	Attributes	Applicable major release
Name: EnvInput4Active (4474) Type: environmentalAlarm Package: equipment.EnvInput4Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput4Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 4 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-174 EnvInput5Active

Alarm	Attributes	Applicable major release
Name: EnvInput5Active (4475) Type: environmentalAlarm Package: equipment.EnvInput5Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput5Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 5 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-175 EnvInput6Active

Alarm	Attributes	Applicable major release
Name: EnvInput6Active (4476) Type: environmentalAlarm Package: equipment.EnvInput6Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput6Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 6 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-176 EnvInput7Active

Alarm	Attributes	Applicable major release
Name: EnvInput7Active (4477) Type: environmentalAlarm Package: equipment.EnvInput7Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput7Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 7 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-177 EnvInput8Active

Alarm	Attributes	Applicable major release
Name: EnvInput8Active (4478) Type: environmentalAlarm Package: equipment.EnvInput8Active Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EnvInput8Active	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Environmental Input 8 active is detected.		
Remedial action: 1. Define the environmental input defined by using one of the following commands: CLI config alm WEBUI Select Reports > Alarm List >Total.		

Table 3-178 EptUploadErr

Alarm	Attributes	Applicable major release
Name: EptUploadErr (5565) Type: communicationsAlarm Package: netw.EptUploadErr Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EptUploadErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when file upload to EPT failed.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-179 EQPTCRYPTO

Alarm	Attributes	Applicable major release
Name: EQPTCRYPTO (4916) Type: configurationAlarm Package: equipment.EQPTCRYPTO Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EQPTCRYPTO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - crypto .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-180 EqptDgrOch

Alarm	Attributes	Applicable major release
Name: EqptDgrOch (3349) Type: communicationsAlarm Package: equipment.EqptDgrOch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgrOch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port degrade - wavelength tracker communication failure is detected.		
Remedial action: This alarm is related to Port Degrade - Wavelength Tracker Communication Failure.1. Perform a warm reset of the card. 2. Perform a cold reset of the card. 3.Resett the card.4. Replace the card.		

Table 3-181 EqptDgrOchOut

Alarm	Attributes	Applicable major release
Name: EqptDgrOchOut (3350) Type: communicationsAlarm Package: equipment.EqptDgrOchOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgrOchOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port degrade - wavelength tracker communication failure is detected.		
Remedial action: This alarm is related to Port Degrade - Wavelength Tracker Communication Failure.1. Perform a warm reset of the card. 2. Perform a cold reset of the card. 3. Reset the card.4. Replace the card.		

Table 3-182 EqptPort

Alarm	Attributes	Applicable major release
Name: EqptPort (3351) Type: equipmentAlarm Package: equipment.EqptPort Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptPort	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port failure - device is detected.		
Remedial action: 1. Perform a warm reset of the card.2. Perform a cold reset of the card.3. Reset the card.4. Remove the pluggable module from the port on the card it is inserted in. Examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage. If no damage is seen, reinsert the pluggable module into its port.5. Remove and replace the pluggable module with another unit of the same type, being careful with the connected fiber jumpers. Refer to Replacing an SFP Module in 1830 Troubleshooting guide.6. Replace the card.		

Table 3-183 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		

Table 3-183 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 3-184 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 3-185 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 3-186 EquipmentFail

Alarm	Attributes	Applicable major release
Name: EquipmentFail (4961) Type: equipmentAlarm Package: rmd.EquipmentFail Raised on class: rmd.Device	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdEQF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is an equipment failure on the RMD Device.		
Remedial action: The failed RMD should be replaced.		

Table 3-187 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-188 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 3-189 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		

Table 3-189 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 3-190 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 3-191 EsCableMismatch1

Alarm	Attributes	Applicable major release
Name: EsCableMismatch1 (5566) Type: communicationsAlarm Package: netw.EsCableMismatch1 Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EsCableMismatch1	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf-1 inter-shelf ES cable mismatch.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-192 ESCLATCHFAIL

Alarm	Attributes	Applicable major release
Name: ESCLATCHFAIL (3720) Type: communicationsAlarm Package: equipment.ESCLATCHFAIL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ESCLATCHFAIL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel attempted escape from latchup routine failed is detected.		

Table 3-192 ESCLATCHFAIL (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1 Check the add or mesh path fibering of the channel for misfibering, kinks or disconnections.2 Check for possible pack failures along the mesh or add paths. If there are any alarms raised, troubleshoot them before continuing with this procedure.3 Perform a Path Power Trace to determine where any possible losses may be occurring.4 Verify that the ingress LD is admin up and is functioning properly. Perform a warm reset of the card if necessary.5 Verify that the CWR8-88, CWR8 or WR8-88A is admin up and functioning properly. If not, perform a warm reset of the card.6 If the alarm is still present, manually set the WSS controller attenuation value by configuring a value at the Sig Out port to set the WSS controller to a more useful attenuation value.7 Once the alarm is cleared, trigger an egress adjustment to optimize the channel powers and Perform a cold reset of the card.8 If the alarm is still present, then provision the NE to the original power settings and then run an egress adjustment.		

Table 3-193 ESM

Alarm	Attributes	Applicable major release
Name: ESM (4400) Type: communicationsAlarm Package: equipment.ESM Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ESM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Encryption State Mismatch is detected.		
Remedial action: Please refer to node Troubleshooting guide for detailed steps for corrective action.		

Table 3-194 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 3-195 EthernetLinkDown

Alarm	Attributes	Applicable major release
Name: EthernetLinkDown (2009) Type: communicationsAlarm Package: equipment.EthernetLinkDown Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Net Applicable probable causes: • Net • LinkDown • NetCraft	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Data Link down is detected.		
Remedial action: This may be caused by the following reasons:1. Damaged or dirty fiber connected to the far-end client equipment receiver.2. Damaged or dirty transmitter inside pluggable module on the far end.3. Problem at the client equipment connected to the far-end OT.4. When EC(ES1 and ES2) and USRPNL(OAMP,VOIP,E1 and E2) are administratively enabled and no Ethernet Link Connectivity Established.		

Table 3-196 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 3-197 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 3-198 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 3-199 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 3-200 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 3-201 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 3-202 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 3-203 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 3-204 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 3-205 EtrMismatch

Alarm	Attributes	Applicable major release
Name: EtrMismatch (4479) Type: equipmentAlarm Package: equipment.EtrMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ETRMISMATCH	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Extended temperature range violation:non-ETR card is detected.		
Remedial action: 1 CLI configure general ETR disabled WEBUI Select System on Equipment Tree, and the System Properties window is displayed. De-select (uncheck) the ETR Validation Enabled field.		

Table 3-206 EtrMismatchMod

Alarm	Attributes	Applicable major release
Name: EtrMismatchMod (3353) Type: equipmentAlarm Package: equipment.EtrMismatchMod Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ETRMISMATCHMOD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Extended temperature range violation:non-ETR Pluggable Module is detected.		
Remedial action: No corrective action is required. This is a normal message.Refer ETR-MISMATCHMOD (Extended Temp Range Violation: non-ETR Pluggable Module) in 1830 Troubleshooting guide for details.		

Table 3-207 ExcessiveCurrentLoad

Alarm	Attributes	Applicable major release
Name: ExcessiveCurrentLoad (2011) Type: equipmentAlarm Package: equipment.ExcessiveCurrentLoad Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExcessLoad	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Excessive Current Load is detected.		

Table 3-207 ExcessiveCurrentLoad (continued)

Alarm	Attributes	Applicable major release
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Remove the pack that is reporting the alarm.2. Do one of the following:Remove load to a level below the capacity of the provisioned power entry cards, or Upgrade the power filters to a higher current capacity (if the supply wiring is sufficiently rated for the current).3. Reprovision the shelf capacity attribute (EXPECTED_AMPS) with the new value.		

Table 3-208 ExcessLoss

Alarm	Attributes	Applicable major release
Name: ExcessLoss (3354) Type: communicationsAlarm Package: equipment.ExcessLoss Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExcessLoss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Fiber connection loss too high is detected.		
Remedial action: 1. Clean or replace fiber, if necessary.		

Table 3-209 EXTIFFAIL

Alarm	Attributes	Applicable major release
Name: EXTIFFAIL (9608) Type: equipmentAlarm Package: equipment.EXTIFFAIL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EXTIFFAIL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when External interface failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-210 FaceplateMissing

Alarm	Attributes	Applicable major release
Name: FaceplateMissing (11086) Type: equipmentAlarm Package: equipment.FaceplateMissing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FaceplateMissing	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Faceplate missing .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-211 FacilityLoopbackConfigured (equipment)

Alarm	Attributes	Applicable major release
Name: FacilityLoopbackConfigured (8380) Type: communicationsAlarm Package: equipment.FacilityLoopbackConfigured Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FacilityLoopbackConfigured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Facility Loopback is configured on Port.		
Remedial action: To clear the condition, disable Facility Loopback configured on port.		

Table 3-212 FAN32HRQD

Alarm	Attributes	Applicable major release
Name: FAN32HRQD (5440) Type: equipmentAlarm Package: equipment.FAN32HRQD Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FAN32HRQD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Require high speed fan (FANH in PSS32) inserted on shelf .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-213 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 3-214 FanSpeedHigh

Alarm	Attributes	Applicable major release
Name: FanSpeedHigh (3356) Type: equipmentAlarm Package: equipment.FanSpeedHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanSpeedHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Fan speed is too high is detected.		
Remedial action: 1. Check for fan obstruction, and clear.2. Reset the fan tray.3. If no problems are found, replace the fan tray.		

Table 3-215 FanSpeedLow

Alarm	Attributes	Applicable major release
Name: FanSpeedLow (3357) Type: equipmentAlarm Package: equipment.FanSpeedLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanSpeedLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Fan speed is too low is detected.		
Remedial action: 1. Check for airflow blockage or a dirty filter, and clear.2. If no problems are found, replace the fan tray.		

Table 3-216 FanSpeedManuallySetMaximum

Alarm	Attributes	Applicable major release
Name: FanSpeedManuallySetMaximum (4480) Type: equipmentAlarm Package: equipment.FanSpeedManuallySetMaximum Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanSpeedMan	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Fan speed manually set to maximum is detected.		
Remedial action: 1. Set the fanspeed parameter to the Normal setting.CLI config fan normal WEBUI Select the Provision/Info button, and view the Details tab. On the Card Properties window, select Normal in the Fan Speed field and click Submit.		

Table 3-217 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 3-218 FarEndLfi

Alarm	Attributes	Applicable major release
Name: FarEndLfi (4481) Type: communicationsAlarm Package: equipment.FarEndLfi Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FeLfi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Local Fault is detected.		

Table 3-218 FarEndLfi (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1 Locate the Far end client OT.2 Proceed with the procedure for clearing LANLFI (see Procedure : Clear LAN Local Fault Indicator.		

Table 3-219 FarEndLos

Alarm	Attributes	Applicable major release
Name: FarEndLos (2016) Type: communicationsAlarm Package: equipment.FarEndLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndLOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Loss of Signal is detected.		
Remedial action: This procedure details the corrective action for clearing FELANLOS against the OT port.1. Locate far end client OT.2. Perform the steps in the procedure LANLOS see PSS Troubleshooting guide for detailed steps.		

Table 3-220 FarEndLossOfSignal

Alarm	Attributes	Applicable major release
Name: FarEndLossOfSignal (2017) Type: communicationsAlarm Package: equipment.FarEndLossOfSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FeLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Loss of Signal is detected.		
Remedial action: This procedure details the corrective action for clearing FELANLOS against the OT port.1. Locate far end client OT.2. Perform the steps in the procedure LANLOS see PSS Troubleshooting guide for detailed steps.		

Table 3-221 FarEndLossOfSynchronization

Alarm	Attributes	Applicable major release
Name: FarEndLossOfSynchronization (4482) Type: communicationsAlarm Package: equipment.FarEndLossOfSynchronization Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FeLss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Loss of Synchronization is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-222 FarEndPortMismatch

Alarm	Attributes	Applicable major release
Name: FarEndPortMismatch (4483) Type: communicationsAlarm Package: equipment.FarEndPortMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FePortMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Port Mapping Mismatch is detected.		
Remedial action: 1 Identify the two ports in the protection group at the near end, and the two ports at the far end.2 Provision the near end and far end ports with the same signal rate and format.3 Provision the timeslot assignments so that the same ports are used at both ends. For example, the near end port C3 must be connected to far end port C3.		

Table 3-223 FarEndRfi

Alarm	Attributes	Applicable major release
Name: FarEndRfi (4484) Type: communicationsAlarm Package: equipment.FarEndRfi Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FeRfi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Far End Remote Fault is detected.		
Remedial action: 1 Locate far end client OT.2 Perform the steps in the procedure Procedure : Clear Remote Fault.3 Proceed with the procedure for clearing LANLFI (see Procedure : Clear LAN Local Fault Indicator.		

Table 3-224 FastPhotonicRestModeMismatch

Alarm	Attributes	Applicable major release
Name: FastPhotonicRestModeMismatch (10280) Type: equipmentAlarm Package: gmpls.FastPhotonicRestModeMismatch Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FastPhotonicRestModeMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an inconsistency in provisioning of the FastPhotonicRestoration parameter is detected.		
Remedial action: Reconfigure FastPhotonicRestoration parameter.		

Table 3-225 Faulty

Alarm	Attributes	Applicable major release
Name: Faulty (3960) Type: communicationsAlarm Package: ptp.Faulty Raised on class: ptp.IEEEPTPPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Faulty	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when PTP port faulty is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-226 FDI

Alarm	Attributes	Applicable major release
Name: FDI (3355) Type: communicationsAlarm Package: equipment.FDI Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FDI	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forward Defect Indication - ODU is detected.		
Remedial action: 1 Check the alarms/conditions along the ODU transmission path.2 Identify the Line alarms in the middle ADM nodes or regenerations nodes (OTU2 LOS,OTU2 LOF).3 Follow the procedure for clearing the identified alarm/condition.4 Refresh the list of current alarms, and check whether the Forward Defect Indication alarm detected on the ODU alarm has cleared.		

Table 3-227 FDICLT

Alarm	Attributes	Applicable major release
Name: FDICLT (3959) Type: communicationsAlarm Package: equipment.FDICLT Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FDICLT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forward Defect Indication-Client Failure is detected.		
Remedial action: Proceed to Procedure - Clear Forward Defect Indication - Client Failure in 1830 Troubleshooting guide.		

Table 3-228 FeasibilityViolation

Alarm	Attributes	Applicable major release
Name: FeasibilityViolation (5567) Type: communicationsAlarm Package: netw.FeasibilityViolation Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FeasibilityViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when optical feasibility violation.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-229 FecEcSignalDegrade

Alarm	Attributes	Applicable major release
Name: FecEcSignalDegrade (2021) Type: communicationsAlarm Package: equipment.FecEcSignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FecEcSd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when PreFEC Signal Degrade is detected.		

Table 3-229 FecEcSignalDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Perform the procedure, DEG (See Troubleshootingguide for details (p. 2-88). Because it is FEC corrected BER, it does not affect service unless another alarm exists on the port. This procedure details the corrective action for a DEG against the OT port. At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Clean the input fiber at the receiver, and check if the input power is within the specified range.2. If it does not clear the alarm, check if there is any power management or optical channel alarm reported on the link. Perform the corrective action for clearing these alarms on the link. 3. Measure the optical signal noise ratio (OSNR) with at the received amplifier with an optical spectrum analyzer. Check if the OSNR is within the range specified by the EPT.Perform the actions to improve the system OSNR. 4. For 40G and 100G coherent cards only: Retrieve the monitoring values for chromatic dispersion (CD), Differential Group Delay (DGD), and Frequency offset. Check if the values are in the normal range. If not, perform the actions to optimize the optical link.		

Table 3-230 FecUbcSignalDegrade

Alarm	Attributes	Applicable major release
Name: FecUbcSignalDegrade (3358) Type: communicationsAlarm Package: equipment.FecUbcSignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fecUbcSd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when PostFEC Signal Degrade is detected.		
Remedial action: This procedure details the corrective action for an FECUBCSD against the OT port. At the end of each step wait to see if the fault clears. If it does not, go to the next step.1. Clean the input fiber at the receiver, and check if the input power is within the specified range.2. Check if there is any power management or optical channel alarm reported on the link. Perform the corrective action for clearing these alarms on the link.3. Measure the optical signal noise ratio (OSNR) with at the received amplifier with an optical spectrum analyzer. Check if the OSNR is within the range specified by the EPT. Perform the actions to improve the system OSNR.		

Table 3-231 FipsFailure

Alarm	Attributes	Applicable major release
Name: FipsFailure (5444) Type: communicationsAlarm Package: equipment.FipsFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FipsFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FIPS Selftest Squelch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-232 FipsSwMismatch

Alarm	Attributes	Applicable major release
Name: FipsSwMismatch (4918) Type: configurationAlarm Package: equipment.FipsSwMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FipsSwMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FIPS Software version mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-233 FirmwarePendingObsolete

Alarm	Attributes	Applicable major release
Name: FirmwarePendingObsolete (2022) Type: equipmentAlarm Package: equipment.FirmwarePendingObsolete Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FwPendingObsolete	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Provisioned firmware will be obsolete after sw upgrade is detected.		
Remedial action: The FWPENDINGOBSOLETE condition is raised against any pack which would be running an obsolete firmware bundle version after the software release upgrade.Provision a firmware bundle that will be valid after software upgrade or provision the default firmware bundle for the card.2. Contact your Nokia support representative.		

Table 3-234 FirmwareUpgradePending

Alarm	Attributes	Applicable major release
Name: FirmwareUpgradePending (2023) Type: equipmentAlarm Package: equipment.FirmwareUpgradePending Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FwUpgradePending	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Firmware upgrade pending is detected.		

Table 3-234 FirmwareUpgradePending (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. To initiate a cold reset to download the recommended firmware version for the affected pack, perform a cold reset of the card.CLI config card card_type shelf slot reset cold WEBUI Select the card, click the Reboot tab, select Cold Reboot >Submit. Note: Refer to Caution at the beginning of this procedure.2. Contact your Nokia support representative.		

Table 3-235 FirmwareVersionNotDefault

Alarm	Attributes	Applicable major release
Name: FirmwareVersionNotDefault (2024) Type: equipmentAlarm Package: equipment.FirmwareVersionNotDefault Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FwVersionNotDefault	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Firmware loaded is not the preferred version is detected.		
Remedial action: 1. Check that the default firmware bundle is provisioned for the card.2. If the default firmware bundle is not provisioned in the previous step, then provision the default firmware bundle for the card.3. Perform a cold reset of the card.4. Contact your Nokia support representative.		

Table 3-236 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-236 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 3-237 FpgaFail

Alarm	Attributes	Applicable major release
Name: FpgaFail (4485) Type: equipmentAlarm Package: equipment.FpgaFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAFAIL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA download failure is detected.		
Remedial action: 1 Perform a warm reset on the card where the FPGAFAIL condition is raised.\nFor CLI config card card type shelf slot reset warm.\nFor WEBUI Select the card, click the Reboot tab, select Warm Reboot >Submit.\n2 Contact your Nokia support representative.		

Table 3-238 FPGAFAILNSA

Alarm	Attributes	Applicable major release
Name: FPGAFAILNSA (5441) Type: communicationsAlarm Package: equipment.FPGAFAILNSA Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAFAILNSA	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA download failure - NSA .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-239 FpgaInit

Alarm	Attributes	Applicable major release
Name: FpgaInit (4486) Type: equipmentAlarm Package: equipment.FpgaInit Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAINIT1 Applicable probable causes: • FPGAINIT1 • FPGAINIT2 • FPGAINIT3 • FPGAINIT4 • FPGAINIT5 • FPGAINIT6 • FPGAINIT7 • FPGAINIT8 • FPGAINIT9 • FPGAINIT10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA initializing is detected.		
Remedial action: 1. No steps are required to clear the FPGAINIT alarm. Some FPGA programming steps can take as long as 45 minutes. Monitor progress using one of the following commands: CLI show firmware upgrade WEBUI Select Reports > Firmware.		

Table 3-240 FPGAINITNSA1

Alarm	Attributes	Applicable major release
Name: FPGAINITNSA1 (5442) Type: communicationsAlarm Package: equipment.FPGAINITNSA1 Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAINITNSA1 Applicable probable causes: • FPGAINITNSA1 • FPGAINITNSA2 • FPGAINITNSA3 • FPGAINITNSA4 • FPGAINITNSA5 • FPGAINITNSA6 • FPGAINITNSA7 • FPGAINITNSA8 • FPGAINITNSA9 • FPGAINITNSA10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA 1 initializing - NSA .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-241 FPGAPRELOAD

Alarm	Attributes	Applicable major release
Name: FPGAPRELOAD (4917) Type: configurationAlarm Package: equipment.FPGAPRELOAD Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAPRELOAD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Preloading portgroup FPGAs .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-242 FpgaTimeout

Alarm	Attributes	Applicable major release
Name: FpgaTimeout (4487) Type: equipmentAlarm Package: equipment.FpgaTimeout Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGATIMEOUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA timeout is detected.		
Remedial action: 1. Perform a warm reset on the card where the FPGATIMEOUT condition is raised.		

Table 3-243 FPGATIMEOUTNSA

Alarm	Attributes	Applicable major release
Name: FPGATIMEOUTNSA (5443) Type: communicationsAlarm Package: equipment.FPGATIMEOUTNSA Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGATIMEOUTNSA	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when FPGA timeout - NSA .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-244 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 3-245 FrcdSwTimRef

Alarm	Attributes	Applicable major release
Name: FrcdSwTimRef (3922) Type: equipmentAlarm Package: optical.FrcdSwTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdSwTimRef	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Forced switch to a timing reference is detected.		

Table 3-245 FrcdSwTimRef (continued)

Alarm	Attributes	Applicable major release
Remedial action: Clear force switch.		

Table 3-246 FrcdSwTimRefT4

Alarm	Attributes	Applicable major release
Name: FrcdSwTimRefT4 (4882) Type: equipmentAlarm Package: optical.FrcdSwTimRefT4 Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrcdSwTimRef_T4	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when T4:Forced switch to a timing reference is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-247 FRCRFCKSEL

Alarm	Attributes	Applicable major release
Name: FRCRFCKSEL (8158) Type: equipmentAlarm Package: equipment.FRCRFCKSEL Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FRCRFCKSEL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Reference Clock - forced switch active.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-248 FrngSync

Alarm	Attributes	Applicable major release
Name: FrngSync (3722) Type: equipmentAlarm Package: equipment.FrngSync Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrngSync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is raised when the system clock is in free-running mode.		
Remedial action: The alarm is raised when system clock in free running mode.Proceed to Procedure -Clear System clock is in free running synchronization mode alarm in 1830 Troubleshooting guide.		

Table 3-249 FRQSLTMISMATCH

Alarm	Attributes	Applicable major release
Name: FRQSLTMISMATCH (9640) Type: equipmentAlarm Package: equipment.FRQSLTMISMATCH Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FRQSLTMISMATCH	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when node detects Och XC widths mismatch along the trail path.		
Remedial action: Och crossconnect spectrail width mismatch detected at this port. Delete and recreate Och Crossconnect with uniform/allowed spectral width along the trail path.		

Table 3-250 FTDEncrypt15Min

Alarm	Attributes	Applicable major release
Name: FTDEncrypt15Min (8159) Type: qualityOfServiceAlarm Package: equipment.FTDEncrypt15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FTD_ENCRYPT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised as indication a FTD ENCRYPT Threshold Crossing detection.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-251 FTDEncrypt1Day

Alarm	Attributes	Applicable major release
Name: FTDEncrypt1Day (8160) Type: qualityOfServiceAlarm Package: equipment.FTDEncrypt1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FTD_ENCRYPT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised as indication a FTD ENCRYPT Threshold Crossing detection.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-252 FwMismatch

Alarm	Attributes	Applicable major release
Name: FwMismatch (5445) Type: communicationsAlarm Package: equipment.FwMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FwMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Firmware version mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-253 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 3-254 GfpExm

Alarm	Attributes	Applicable major release
Name: GfpExm (8432) Type: equipmentAlarm Package: equipment.GfpExm Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpExm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-254 GfpExm (continued)

Alarm	Attributes	Applicable major release
Description: GFP Extension Header Mismatch		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-255 GfpLof

Alarm	Attributes	Applicable major release
Name: GfpLof (5176) Type: communicationsAlarm Package: equipment.GfpLof Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpLof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of GFP alignment occurs.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-256 GfpLofOut

Alarm	Attributes	Applicable major release
Name: GfpLofOut (4488) Type: communicationsAlarm Package: equipment.GfpLofOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpLofOut Applicable probable causes: • GfpLofOut • GFPLOF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Loss of GFP alignment is detected.		
Remedial action: Refer Procedure : Clear Loss of GFP alignment in 1830 Troubleshooting guide.		

Table 3-257 GfpUpm

Alarm	Attributes	Applicable major release
Name: GfpUpm (4919) Type: communicationsAlarm Package: equipment.GfpUpm Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpUpm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GFP User Payload Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-258 GmreDegraded

Alarm	Attributes	Applicable major release
Name: GmreDegraded (8222) Type: equipmentAlarm Package: gmpls.GmreDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is not fully operational.		
Remedial action: Not Available.		

Table 3-259 GmreInAutomaticRestorationDisabledMode

Alarm	Attributes	Applicable major release
Name: GmreInAutomaticRestorationDisabledMode (8223) Type: equipmentAlarm Package: gmpls. GmreInAutomaticRestorationDisabledMode Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreInAutomaticRestora-tionDisabledMode	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is set to manual restoration by operator.		
Remedial action: Not Available.		

Table 3-260 GmreInMigration

Alarm	Attributes	Applicable major release
Name: GmreInMigration (8224) Type: equipmentAlarm Package: gmpls.GmreInMigration Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmreInMigration	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE is in Migration.		
Remedial action: Not Available.		

Table 3-261 HighBer

Alarm	Attributes	Applicable major release
Name: HighBer (4489) Type: communicationsAlarm Package: equipment.HighBer Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HiBer	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when High BER is detected.		
Remedial action: 1 Retrieve power level reading on the local OT port.2 Clean the fiber.3 If cleaning the fiber does not clear the problem, replace the fiber.4 If the power level is within the operating range, check for pluggable module alarms.5 Replace the pluggable module		

Table 3-262 HiRamanGain

Alarm	Attributes	Applicable major release
Name: HiRamanGain (9040) Type: communicationsAlarm Package: equipment.HiRamanGain Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HiRamanGain	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Raman Gain too high .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-263 HldOvrSync

Alarm	Attributes	Applicable major release
Name: HldOvrSync (3917) Type: equipmentAlarm Package: equipment.HldOvrSync Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HldOvrSync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the system clock is in hold-over mode.		
Remedial action: Check all references.		

Table 3-264 HpPlmP

Alarm	Attributes	Applicable major release
Name: HpPlmP (4490) Type: communicationsAlarm Package: equipment.HpPlmP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HpPlmP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when HP PLM PATH is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-265 HpRdiP

Alarm	Attributes	Applicable major release
Name: HpRdiP (3723) Type: communicationsAlarm Package: equipment.HpRdiP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HpRdiP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when HP RDI PATH is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-266 HpUneqP

Alarm	Attributes	Applicable major release
Name: HpUneqP (4491) Type: communicationsAlarm Package: equipment.HpUneqP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HpUneqP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when HP UNEQ PATH is detected.		
Remedial action: Proceed as follows to clear an HOPath Unequipped alarm:1 Define the cross-connections consistently at both ends of the path.		

Table 3-267 HwAccessFailure

Alarm	Attributes	Applicable major release
Name: HwAccessFailure (8433) Type: equipmentAlarm Package: equipment.HwAccessFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HwAccessFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Hardware device access failure.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-268 HwRevisionNotSupported

Alarm	Attributes	Applicable major release
Name: HwRevisionNotSupported (2032) Type: equipmentAlarm Package: equipment.HwRevisionNotSupported Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HwRevisionNotSupported	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Hardware not supported for current configuration is detected.		
Remedial action: 1. Replace the affected Equipment Controller. Refer to 1830 Troubleshooting guide - Replacing an Equipment Controller in a Redundant Shelf for the complete trouble-clearing procedure.		

Table 3-269 HwrvUnknown

Alarm	Attributes	Applicable major release
Name: HwrvUnknown (11088) Type: equipmentAlarm Package: equipment.HwrvUnknown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HwrvUnknown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: SW/FW not contained in this release - card will not boot.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-270 ImageNotReady

Alarm	Attributes	Applicable major release
Name: ImageNotReady (5446) Type: communicationsAlarm Package: equipment.ImageNotReady Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ImageNotReady	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card Image Not Installed .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-271 InBandCommDegraded

Alarm	Attributes	Applicable major release
Name: InBandCommDegraded (8225) Type: communicationsAlarm Package: gmpls.InBandCommDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandCommDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a problem on at least one ECC channel of the ECC protection group. The ECC channel might be not protected anymore.		
Remedial action: Not Available.		

Table 3-272 InBandCommDown

Alarm	Attributes	Applicable major release
Name: InBandCommDown (8226) Type: communicationsAlarm Package: gmpls.InBandCommDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandCommDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP communication via the ECC protection group is not working.		
Remedial action: Not Available.		

Table 3-273 IncomingSupvyLof

Alarm	Attributes	Applicable major release
Name: IncomingSupvyLof (4493) Type: communicationsAlarm Package: equipment.IncomingSupvyLof Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LofO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Incoming SUPVY LOF is detected.		
Remedial action: Refer Procedure : Clear Incoming SUPVY LOF in 1830 Troubleshooting guide.		

Table 3-274 IncomingSupvyLos

Alarm	Attributes	Applicable major release
Name: IncomingSupvyLos (4494) Type: communicationsAlarm Package: equipment.IncomingSupvyLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Incoming SUPVY LOS is detected.		
Remedial action: Refer Procedure : Clear Incoming SUPVY LOS in 1830 Troubleshooting guide.		

Table 3-275 IncompatFan

Alarm	Attributes	Applicable major release
Name: IncompatFan (3359) Type: equipmentAlarm Package: equipment.IncompatFan Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompatFan	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Incompatible Fan is detected.		
Remedial action: No corrective action is required. This is a normal message.For replacing Fan refer to 1830 Troubleshooting guide.		

Table 3-276 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 3-277 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 3-278 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 3-279 InMaintenance

Alarm	Attributes	Applicable major release
Name: InMaintenance (4492) Type: equipmentAlarm Package: equipment.InMaintenance Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Man	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manually caused abnormal condition - card in maintenance is detected.		
Remedial action: Proceed as follows to clear the Manually caused abnormal condition - card in maintenance alarm.1 Manually place the card in service using the following command:CLI config slot shelf slot state up.		

Table 3-280 InMigration

Alarm	Attributes	Applicable major release
Name: InMigration (5568) Type: communicationsAlarm Package: netw.InMigration Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InMigration	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE in migration.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-281 InterCardCommsFailure

Alarm	Attributes	Applicable major release
Name: InterCardCommsFailure (2036) Type: equipmentAlarm Package: equipment.InterCardCommsFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ContCom	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card failure - communication is detected.		
Remedial action: Please refer CONTCOM (Card Failure - Communication) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-282 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 3-283 InterShelfLossofComms

Alarm	Attributes	Applicable major release
Name: InterShelfLossofComms (4495) Type: equipmentAlarm Package: equipment.InterShelfLossofComms Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ContCom	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-283 InterShelfLossofComms (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Inter-shelf loss of communication is detected.		
Remedial action: Refer Procedure : Clear Inter-shelf loss of communication alarm in 1830 Troubleshooting guide.		

Table 3-284 IntOhFail

Alarm	Attributes	Applicable major release
Name: IntOhFail (11091) Type: communicationsAlarm Package: equipment.IntOhFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntOhFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal overhead failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-285 Intrusion

Alarm	Attributes	Applicable major release
Name: Intrusion (3601) Type: communicationsAlarm Package: netw.Intrusion Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Intrusion	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when excessive invalid login attempts by users is detected.		
Remedial action: To clear the INTRUSION alarm, complete either Step 1 OR Step 2.1.Disable the user in the User Security Database.2. Delete the user in the User Security Database.		

Table 3-286 IntTempHigh

Alarm	Attributes	Applicable major release
Name: IntTempHigh (3360) Type: equipmentAlarm Package: equipment.IntTempHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card over temperature is detected.		

Table 3-286 IntTempHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the steps in the procedure - High Temperature Troubleshooting.1. Verify that the fan tray is installed and that no fan tray alarms are present.Correct any faults found.2. Visually inspect the shelf to confirm that filler cards are installed in all empty slots in the shelf. This helps ensure proper airflow.3. Check for a dirty air filter. Clean or replace it as necessary. Contact your service representative for replacement filters.4. Use a thermometer to measure the ambient air temperature at the intake of the fans. Verify that the ambient temperature is not abnormally high. If the ambient temperature is too high, the NE may require additional cooling to bring it back to an acceptable operating temperature.5. Verify if other cards in the shelf report temperatures near their upper limit (within 10 ï¿½C).6. Replace the card and follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 3-287 IntTempLow

Alarm	Attributes	Applicable major release
Name: IntTempLow (3361) Type: equipmentAlarm Package: equipment.IntTempLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card under temperature is detected.		
Remedial action: Ensure that no environmental issues are present where the network element resides.Resolve any existing issues.Verify if other cards in the shelf report temperatures near their lower limit (within 10ï¿½ C).Replace the alarmed card.		

Table 3-288 IntTempOpt

Alarm	Attributes	Applicable major release
Name: IntTempOpt (3362) Type: equipmentAlarm Package: equipment.IntTempOpt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempOpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optics over temperature is detected.		
Remedial action: Steps for High Temperature Troubleshooting.1. Verify that the fan tray is installed and that no fan tray alarms are present.Correct any faults found.2. Visually inspect the shelf to confirm that filler cards are installed in all empty slots in the shelf. This helps ensure proper airflow.3. Check for a dirty air filter. Clean or replace it as necessary. Contact your service representative for replacement filters.4. Use a thermometer to measure the ambient air temperature at the intake of the fans. Verify that the ambient temperature is not abnormally high. If the ambient temperature is too high, the NE may require additional cooling to bring it back to an acceptable operating temperature.5. Verify if other cards in the shelf report temperatures near their upper limit (within 10 ï¿½C).6. Replace the card and follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 3-289 IntTsiFailure

Alarm	Attributes	Applicable major release
Name: IntTsiFailure (11092) Type: equipmentAlarm Package: equipment.IntTsiFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: INTTSIFAIL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-289 IntTsiFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Internal timeslot interchange failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-290 InvalidEgress

Alarm	Attributes	Applicable major release
Name: InvalidEgress (3363) Type: equipmentAlarm Package: equipment.InvalidEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid or no egress port defined is detected.		
Remedial action: Check the topology between ingress and egress LD (if there is egress LD). Check the external topology for the ingress LD line port. If the topology is missing, add the topology and re-run the egress adjustment.Ensure that Opposite Direction Port field is provisioned correctly for the egress LD Lineout port.		

Table 3-291 InvalidModule

Alarm	Attributes	Applicable major release
Name: InvalidModule (11093) Type: equipmentAlarm Package: equipment.InvalidModule Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidModule	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid Pluggable Module .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-292 InvalidThreshold

Alarm	Attributes	Applicable major release
Name: InvalidThreshold (2038) Type: communicationsAlarm Package: equipment.InvalidThreshold Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidThreshold	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid Threshold is detected.		
Remedial action: 1. Determine whether the threshold calculation is in automatic or manual mode.2. Is manual switch calculation mode is in effect? (The default is auto.).3. Verify that no LOS alarms are present on the A or B input ports that would inhibit the switch calculation.4. Set the threshold to a value greater than -30 dBm based on engineering rules for the incoming channel power levels.5. STOP,You have completed this procedure.		

Table 3-293 InvalidThresholdOms

Alarm	Attributes	Applicable major release
Name: InvalidThresholdOms (3364) Type: communicationsAlarm Package: equipment.InvalidThresholdOms Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidThresholdOms	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid Threshold - OMS is detected.		
Remedial action: 1. Determine whether the threshold calculation is in automatic or manual mode.2. Is manual switch calculation mode is in effect? (The default is auto.).3. Verify that no LOS alarms are present on the A or B input ports that would inhibit the switch calculation.4. Set the threshold to a value greater than -30 dBm based on engineering rules for the incoming channel power levels.5. STOP,You have completed this procedure. Please refer 1830 Troubleshooting guide for further details.		

Table 3-294 InvalidThresholdOts

Alarm	Attributes	Applicable major release
Name: InvalidThresholdOts (3365) Type: communicationsAlarm Package: equipment.InvalidThresholdOts Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidThresholdOts	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid Threshold - OTS is detected.		

Table 3-294 InvalidThresholdOts (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Determine whether the threshold calculation is in automatic or manual mode.2. Is manual switch calculation mode is in effect? (The default is auto.).3. Verify that no LOS alarms are present on the A or B input ports that would inhibit the switch calculation.4. Set the threshold to a value greater than -30 dBm based on engineering rules for the incoming channel power levels.5. STOP,You have completed this procedure. Please refer 1830 Troubleshooting guide for further details.		

Table 3-295 InvalidXc

Alarm	Attributes	Applicable major release
Name: InvalidXc (11094) Type: communicationsAlarm Package: equipment.InvalidXc Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidXc	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid Cross Connection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-296 InventoryErrMod

Alarm	Attributes	Applicable major release
Name: InventoryErrMod (11095) Type: equipmentAlarm Package: equipment.InventoryErrMod Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InventoryErrMod	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module Inventory Error .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-297 InventoryError

Alarm	Attributes	Applicable major release
Name: InventoryError (3724) Type: equipmentAlarm Package: equipment.InventoryError Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InventoryError Applicable probable causes: • InventoryError • CFCAPACITYWARNING	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card Inventory Error is detected.		
Remedial action: To clear the INVENTORYERROR alarm, remove and replace the affected device.		

Table 3-298 KeyDomainErr

Alarm	Attributes	Applicable major release
Name: KeyDomainErr (5177) Type: communicationsAlarm Package: equipment.KeyDomainErr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyDomainErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Wavelength tracker domain provisioning error occurs.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-299 LagDeg

Alarm	Attributes	Applicable major release
Name: LagDeg (3961) Type: communicationsAlarm Package: equipment.LagDeg Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LagDeg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Link aggregation group signal degrade is detected.		
Remedial action: Please refer section - Signal Degrade 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-300 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 3-301 LagLos

Alarm	Attributes	Applicable major release
Name: LagLos (3962) Type: communicationsAlarm Package: equipment.LagLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LagLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Link aggregation group Loss of Signal is detected.		

Table 3-301 LagLos (continued)

Alarm	Attributes	Applicable major release
Remedial action: Proceed as follows to clear the Link Aggregation Group Loss of Signal alarm.1.Ensure that the administrative state of the Link Aggregation Group is Admin Up.2.Ensure that the Max Port Size of the Link Aggregation Group is larger than 0.3.Ensure that the number of attached ports in the Link Aggregation Group is larger than 0.4.Check the alarms/conditions of the attached port.5.Follow the procedure for clearing the identified alarm/condition of the attached port.6.Refresh the list of current alarms , and check whether Link Aggregation Group Loss of Signal has cleared.		

Table 3-302 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 3-303 LanLol

Alarm	Attributes	Applicable major release
Name: LanLol (4499) Type: communicationsAlarm Package: equipment.LanLol Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanLol Applicable probable causes: • LanLol • LOL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Link is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-304 LanSf

Alarm	Attributes	Applicable major release
Name: LanSf (3725) Type: communicationsAlarm Package: equipment.LanSf Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanSf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when LAN Signal Failure is detected.		
Remedial action: Signal Failure alarm.Please refer 1830 Troubleshooting guide for detailed corrective action.		

Table 3-305 LaserBackFacetOptPwrTca

Alarm	Attributes	Applicable major release
Name: LaserBackFacetOptPwrTca (3366) Type: communicationsAlarm Package: equipment.LaserBackFacetOptPwrTca Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LaserBackFacetOptPwrTca	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Laser back-facet optical power cross threshold is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. If another card failure is reported on the card, follow the procedure for that specific alarm.2. If the port is pluggable module, remove and reinsert the same module. If the alarm does not clear, replace the module.		

Table 3-306 LaserCoolingCurTca

Alarm	Attributes	Applicable major release
Name: LaserCoolingCurTca (3367) Type: communicationsAlarm Package: equipment.LaserCoolingCurTca Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LaserCoolingCurTca	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Laser cooling current cross threshold is detected.		

Table 3-306 LaserCoolingCurTca (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm corresponds to Laser Cooling Current Cross Threshold.1. If another card failure is reported on the card, follow the procedure for that specific alarm.2. If the port is pluggable module, remove and reinsert the same module. If the alarm does not clear, replace the module.		

Table 3-307 LaserEndOfLife

Alarm	Attributes	Applicable major release
Name: LaserEndOfLife (2039) Type: equipmentAlarm Package: equipment.LaserEndOfLife Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LaserEOL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Laser end of life is detected.		
Remedial action: The OT port has detected laser end of life.If another card failure is reported on the card, follow the procedure for that specific alarm.If the port is pluggable module, remove and reinsert the same module. If the alarm does not clear, replace the module.		

Table 3-308 LatchOpen

Alarm	Attributes	Applicable major release
Name: LatchOpen (5630) Type: equipmentAlarm Package: equipment.LatchOpen Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LATCHOPEN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one of the latches is not closed .		
Remedial action: Indicates that one of the latches are not closed.Close the Latch		

Table 3-309 LckOut

Alarm	Attributes	Applicable major release
Name: LckOut (4500) Type: communicationsAlarm Package: equipment.LckOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LckOut Applicable probable causes: • LckOut • LCK	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Locked - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-310 LfiEgress

Alarm	Attributes	Applicable major release
Name: LfiEgress (4501) Type: communicationsAlarm Package: equipment.LfiEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LfiEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Client Local Fault is detected.		
Remedial action: 1 Locate far end OT.2 Perform the steps in the procedure Procedure : Clear LAN Local Fault Indicator on the far end port in 1830 Troubleshooting guide.		

Table 3-311 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		

Table 3-311 LicensedLimitExceeded (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 3-312 LineFacilityLoopbackActive

Alarm	Attributes	Applicable major release
Name: LineFacilityLoopbackActive (4502) Type: equipmentAlarm Package: equipment.LineFacilityLoopbackActive Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LpbkLine	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Line Facility loopback active is detected.		
Remedial action: 1 Remove the loopback from the port.For CLI config interface <shelf slot port> loopback line disabled		

Table 3-313 LinkDiversityViolation

Alarm	Attributes	Applicable major release
Name: LinkDiversityViolation (8228) Type: communicationsAlarm Package: gmpls.LinkDiversityViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LinkDiversityViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no fully link-diverse backup route could be found for the current route of the LSP.		
Remedial action: Not Available.		

Table 3-314 LinkDiviersity

Alarm	Attributes	Applicable major release
Name: LinkDiviersity (5569) Type: communicationsAlarm Package: netw.LinkDiviersity Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LinkDiviersity	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when link diversity violation.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-315 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 3-316 LnkSpdDeg

Alarm	Attributes	Applicable major release
Name: LnkSpdDeg (11096) Type: equipmentAlarm Package: equipment.LnkSpdDeg Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LnkSpdDeg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Link speed degraded .		

Table 3-316 LnkSpdDeg (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-317 Loam

Alarm	Attributes	Applicable major release
Name: Loam (3368) Type: communicationsAlarm Package: equipment.Loam Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOAM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Alignment Marker Lock is detected.		
Remedial action: The LOAM condition is raised when the system cannot detect the PCS lane marker, or the marker has been displaced.Replace the CFP.		

Table 3-318 LocalFault

Alarm	Attributes	Applicable major release
Name: LocalFault (2041) Type: communicationsAlarm Package: equipment.LocalFault Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanLfi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Local Fault is detected.		
Remedial action: 1. Locate the Far end client OT.2. Proceed with the procedure for clearing LANLFI.		

Table 3-319 LocalPacketLost

Alarm	Attributes	Applicable major release
Name: LocalPacketLost (5592) Type: communicationsAlarm Package: rmd.LocalPacketLost Raised on class: rmd.TsopChannel	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdTsopLPL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no packets are received for one second. Cleared when two contiguous packets are received.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-320 LockedIndication

Alarm	Attributes	Applicable major release
Name: LockedIndication (4503) Type: communicationsAlarm Package: equipment.LockedIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lck Applicable probable causes: • Lck • LockedIndicationEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Locked Indication is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-321 LockedIndicationEgress

Alarm	Attributes	Applicable major release
Name: LockedIndicationEgress (4920) Type: communicationsAlarm Package: equipment.LockedIndicationEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LockedIndicationEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Locked Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-322 LockoutOfTimRef

Alarm	Attributes	Applicable major release
Name: LockoutOfTimRef (3923) Type: equipmentAlarm Package: optical.LockoutOfTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LockoutOfTimRef	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Lock out of a timing reference is detected.		
Remedial action: Check the timing reference quality and priority.		

Table 3-323 LockoutOfTimRefT4

Alarm	Attributes	Applicable major release
Name: LockoutOfTimRefT4 (4883) Type: equipmentAlarm Package: optical.LockoutOfTimRefT4 Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LockoutOfTimRef_T4	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when T4:Lock out of a timing reference is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-324 LOFLOM

Alarm	Attributes	Applicable major release
Name: LOFLOM (4496) Type: communicationsAlarm Package: equipment.LOFLOM Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOFLOM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU LOFLOM is detected.		
Remedial action: Refer Procedure : Clear Loss of Frame and Loss of Multiframe in 1830 Troubleshooting guide.		

Table 3-325 LOFLOMOut

Alarm	Attributes	Applicable major release
Name: LOFLOMOut (4497) Type: communicationsAlarm Package: equipment.LOFLOMOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOFLOMOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU LOFLOM OUT is detected.		
Remedial action: Refer Procedure : Clear Loss of Frame and Loss of Multiframe in 1830 Troubleshooting guide.		

Table 3-326 Lol

Alarm	Attributes	Applicable major release
Name: Lol (4504) Type: communicationsAlarm Package: equipment.Lol Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lol	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Lane Alignment is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-327 LOLA

Alarm	Attributes	Applicable major release
Name: LOLA (8163) Type: communicationsAlarm Package: equipment.LOLA Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOLA	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Lane Alignment.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-328 LOOMFI

Alarm	Attributes	Applicable major release
Name: LOOMFI (8434) Type: equipmentAlarm Package: equipment.LOOMFI Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOOMFI	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: ODU LOOMFI		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-329 LoRamanGain

Alarm	Attributes	Applicable major release
Name: LoRamanGain (9041) Type: communicationsAlarm Package: equipment.LoRamanGain Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoRamanGain	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Raman Gain too low .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-330 LosDcm

Alarm	Attributes	Applicable major release
Name: LosDcm (4505) Type: communicationsAlarm Package: equipment.LosDcm Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosDcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when From DCM Input LOS is detected.		
Remedial action: Refer Procedure : Clear From DCM Input LOS in 1830 Troubleshooting guide.		

Table 3-331 LOSEDFA

Alarm	Attributes	Applicable major release
Name: LOSEDFA (4498) Type: communicationsAlarm Package: equipment.LOSEDFA Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOSEDFA	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when EDFA Input LOS is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-332 LOSN1

Alarm	Attributes	Applicable major release
Name: LOSN1 (8435) Type: equipmentAlarm Package: equipment.LOSN1 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOSN1	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Loss of Signal from N+1		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-333 LOSN2

Alarm	Attributes	Applicable major release
Name: LOSN2 (8436) Type: equipmentAlarm Package: equipment.LOSN2 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOSN2	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Loss of Signal from N+2		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-334 LOSOAMP

Alarm	Attributes	Applicable major release
Name: LOSOAMP (5447) Type: communicationsAlarm Package: equipment.LOSOAMP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOSOAMP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SUPVY Amplifier Input LOS .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-335 LosOcm

Alarm	Attributes	Applicable major release
Name: LosOcm (3370) Type: communicationsAlarm Package: equipment.LosOcm Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosOcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when WTOCM Input LOS is detected.		
Remedial action: 1. Verify the fiber is connected between the WTOCM input port and its associated LD MON port.2. Verify there is no existing LOS condition on the associated LD card. 3. Retrieve power level reading on the local port, verify the power in within the normal operating range.4. Clean the fiber.5. Replace the fiber.6. Replace the pluggable module.		

Table 3-336 LosOms

Alarm	Attributes	Applicable major release
Name: LosOms (3371) Type: communicationsAlarm Package: equipment.LosOms Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosOms	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		
Remedial action: Please refer LOS-P (Incoming Payload LOS) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-337 LosOOut

Alarm	Attributes	Applicable major release
Name: LosOOut (3369) Type: communicationsAlarm Package: equipment.LosOOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOSOOUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing SUPVY LOS is detected.		
Remedial action: Please refer LOS-OUT (Outgoing Loss of Signal) and (Outgoing Channel Absent) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-338 LosOts

Alarm	Attributes	Applicable major release
Name: LosOts (3372) Type: communicationsAlarm Package: equipment.LosOts Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosOts Applicable probable causes: • LosOts • LOSOTS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OPS Input Loss of Signal is detected.		
Remedial action: Please refer LOS-P (Incoming Payload LOS) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-339 LosP

Alarm	Attributes	Applicable major release
Name: LosP (4921) Type: communicationsAlarm Package: equipment.LosP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal - OTU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-340 LossOfClock (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: equipment.LossOfClock Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LostClock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of clock is detected.		
Remedial action: This demerit is raised when a shelf controller determines that there is no system timing clock from the master shelf. This demerit will cause a controller activity switch if the inactive controller does not have this demerit raised, but the active does.		

Table 3-341 LossOfFrame (optical)

Alarm	Attributes	Applicable major release
Name: LossOfFrame (630) Type: communicationsAlarm Package: optical.LossOfFrame Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lof Applicable probable causes: • Lof • LOF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer 1830 PSS Node Maintenance manual for remedial action information.		

Table 3-342 LossOfFrameDelineation

Alarm	Attributes	Applicable major release
Name: LossOfFrameDelineation (4506) Type: communicationsAlarm Package: equipment.LossOfFrameDelineation Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lfd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GFP Loss of Frame Delineation is detected.		
Remedial action: 1 Inspect the OCh trail which is used as a server transport layer for GFP stream.2 If any alarms are detected on OCh trail, locate the farthest upstream point and follow the procedure for clearing this alarm.3 Locate the far end OT that sources the GFP stream.4 Perform a soft reset of both local and far-end OT.5 If Step 4 does not clear the problem replace far-end OT.6 If Step 5 does not clear the problem replace the local OT.		

Table 3-343 LossOfFrameEgress

Alarm	Attributes	Applicable major release
Name: LossOfFrameEgress (4507) Type: communicationsAlarm Package: equipment.LossOfFrameEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LofEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Frame Egress is detected.		

Table 3-343 LossOfFrameEgress (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1 Locate far end OT.2 Perform the steps in the procedureProcedure : Clear Loss Of Frame (photonic applications) on the far end port.		

Table 3-344 LossOfLock

Alarm	Attributes	Applicable major release
Name: LossOfLock (4886) Type: communicationsAlarm Package: ptp.LossOfLock Raised on class: ptp.IEEEPTPClock	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfLock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of 1588 synchronization is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-345 LossOfOpticalSignal

Alarm	Attributes	Applicable major release
Name: LossOfOpticalSignal (5593) Type: equipmentAlarm Package: rmd.LossOfOpticalSignal Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfLOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ingress TDM defects LOS, for example fiber is missing or broken, or the connector is dirty		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-346 LossOfPrimaryLineTimingClock

Alarm	Attributes	Applicable major release
Name: LossOfPrimaryLineTimingClock (4508) Type: equipmentAlarm Package: equipment.LossOfPrimaryLineTimingClock Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of primary line timing recovered clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-347 LossOfSecondaryLineTimingClock

Alarm	Attributes	Applicable major release
Name: LossOfSecondaryLineTimingClock (4509) Type: equipmentAlarm Package: equipment. LossOfSecondaryLineTimingClock Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of secondary line timing recovered clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-348 LossOfSignal (optical)

Alarm	Attributes	Applicable major release
Name: LossOfSignal (631) Type: communicationsAlarm Package: optical.LossOfSignal Raised on class: optical.OpticalPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los Applicable probable causes: • Los • LosP • LosOut • LosLdSig • LanLos • LOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		
Remedial action: A receive port on one of the optical cards has detected a loss of signal. The LOS condition may be raised for the following reasons:1. a misconnected, damaged, or dirty fiber.2. the received power may not be within the acceptable range.The procedures in this section are as follows:1. LOS (Channel Absent Alarm) 2. LD Input LOS.3. CWR Input LOS.4. LOS (Loss of Signal.Please refer detailed section for each in 1830 Troubleshooting guide.		

Table 3-349 LossOfSignalC

Alarm	Attributes	Applicable major release
Name: LossOfSignalC (11097) Type: communicationsAlarm Package: equipment.LossOfSignalC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosPC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Incoming Payload LOS C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-350 LossOfSignalL

Alarm	Attributes	Applicable major release
Name: LossOfSignalL (11098) Type: communicationsAlarm Package: equipment.LossOfSignalL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LosPL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Incoming Payload LOS L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-351 LossOfSonetSdhFrame

Alarm	Attributes	Applicable major release
Name: LossOfSonetSdhFrame (5594) Type: equipmentAlarm Package: rmd.LossOfSonetSdhFrame Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdNimLOF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is optical power, but the signal is not SONET/SDH framed..		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-352 LossOfSync

Alarm	Attributes	Applicable major release
Name: LossOfSync (4510) Type: communicationsAlarm Package: equipment.LossOfSync Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lss Applicable probable causes: • Lss • LSS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of synchronization is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-353 LossOfSynchronizationEgress

Alarm	Attributes	Applicable major release
Name: LossOfSynchronizationEgress (4511) Type: communicationsAlarm Package: equipment.LossOfSynchronizationEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LssEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Client Loss of Synchronization is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-354 LossTooHigh

Alarm	Attributes	Applicable major release
Name: LossTooHigh (3373) Type: communicationsAlarm Package: equipment.LossTooHigh Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprLossHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - loss too high is detected.		
Remedial action: Please refer OPRLOSSHIGH (Out of Operational Range Loss Too High between DCM Ports of LD) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-355 LossTooLow

Alarm	Attributes	Applicable major release
Name: LossTooLow (2042) Type: equipmentAlarm Package: equipment.LossTooLow Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprLossLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - loss too low is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Perform a lightpath trace to check the upstream power levels, making sure that the expected powers are met. Clean fiber connections if necessary and make sure fibers are not kinked or pinched.2. Check if there are any other existing power-related alarms at the amplifier card, and troubleshoot them first.3. Retrieve the optical power levels at the DCM port of the amplifier card where the alarm is raised.WEBUI From the Equipment Tree, select the card, and select the desired port.4. Perform a warm reset on the card where the OPR condition is raised.5. Perform a cold reset of the card.6. Reseat the card.7. Replace the card. Follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 3-356 LostBothTimingReferences

Alarm	Attributes	Applicable major release
Name: LostBothTimingReferences (4858) Type: equipmentAlarm Package: netw.LostBothTimingReferences Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncOos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-356 LostBothTimingReferences (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when System timing lost both references is detected.		
Remedial action: Please refer section SYNCOOS (Timing reference failed (Not Protected or Protection not Available)) / SYNCOOS (Timing reference failed--system going into holdover) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-357 LostRedundantTimingReference

Alarm	Attributes	Applicable major release
Name: LostRedundantTimingReference (4859) Type: equipmentAlarm Package: netw.LostRedundantTimingReference Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing lost a redundant reference is detected.		
Remedial action: The alarm is raised due to lost of redundant reference of system time.Refer SYNC section in in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-358 LotOut

Alarm	Attributes	Applicable major release
Name: LotOut (3726) Type: communicationsAlarm Package: equipment.LotOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LotOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Loss of tones is detected.		
Remedial action: Please refer section LOT-OUT (Outgoing Loss of Tones) and Path Power Trace for detailed steps to clear the alarm.		

Table 3-359 LotOutC

Alarm	Attributes	Applicable major release
Name: LotOutC (11099) Type: communicationsAlarm Package: equipment.LotOutC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LotOutC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Loss of tones C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-360 LotOutL

Alarm	Attributes	Applicable major release
Name: LotOutL (11100) Type: communicationsAlarm Package: equipment.LotOutL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LotOutL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Loss of tones L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-361 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 3-361 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 3-362 LspFailedApe

Alarm	Attributes	Applicable major release
Name: LspFailedApe (5570) Type: communicationsAlarm Package: netw.LspFailedApe Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspFailedApe	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Active failed - APE failed.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-363 LspFailedPre

Alarm	Attributes	Applicable major release
Name: LspFailedPre (5571) Type: communicationsAlarm Package: netw.LspFailedPre Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspFailedPre	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when active failed - preemption.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-364 LspFailedTp

Alarm	Attributes	Applicable major release
Name: LspFailedTp (5572) Type: communicationsAlarm Package: netw.LspFailedTp Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspFailedTp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when active failed - transmission problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-365 LspFailedUnprot

Alarm	Attributes	Applicable major release
Name: LspFailedUnprot (5573) Type: communicationsAlarm Package: netw.LspFailedUnprot Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspFailedUnprot	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when active failed - unprotected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-366 LspFailedXc

Alarm	Attributes	Applicable major release
Name: LspFailedXc (5574) Type: communicationsAlarm Package: netw.LspFailedXc Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspFailedXc	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when active failed - cross connection problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-367 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 3-368 ManLR

Alarm	Attributes	Applicable major release
Name: ManLR (4884) Type: equipmentAlarm Package: optical.ManLR Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManLR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Logical removal of a timing reference is detected.		
Remedial action: To clear the condition, check with the assigning of connection between the LINEREF and the physical port.		

Table 3-369 ManSwTimRef

Alarm	Attributes	Applicable major release
Name: ManSwTimRef (3925) Type: equipmentAlarm Package: optical.ManSwTimRef Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManSwTimRef	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Manual switch to a timing reference is detected.		
Remedial action: Check the timing reference quality and priority.		

Table 3-370 ManSwTimRefT4

Alarm	Attributes	Applicable major release
Name: ManSwTimRefT4 (4885) Type: equipmentAlarm Package: optical.ManSwTimRefT4 Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManSwTimRef_T4	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when T4:Manual switch to a timing reference is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-371 ManSwToInt

Alarm	Attributes	Applicable major release
Name: ManSwToInt (3918) Type: equipmentAlarm Package: equipment.ManSwToInt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ManSwToInt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System clock forced to internal clock is detected.		
Remedial action: Clear the manual switch.		

Table 3-372 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 3-373 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 3-374 MepError

Alarm	Attributes	Applicable major release
Name: MepError (5508) Type: oamAlarm Package: ethernetoam.MepError Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MepError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when MEP Error CCM is detected.		
Remedial action: Ensure that all expected peer MEPs are configured correctly.		

Table 3-375 MepLoc

Alarm	Attributes	Applicable major release
Name: MepLoc (3727) Type: oamAlarm Package: ethernetoam.MepLoc Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Loc	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP stops receiving CCM frames from a peer MEP.		
Remedial action: This alarm is raised when a MEP stops receiving CCM frames from the peer MEP.		

Table 3-376 MepMacError

Alarm	Attributes	Applicable major release
Name: MepMacError (5509) Type: oamAlarm Package: ethernetoam.MepMacError Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MepMacError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when MEP Mac Status is detected.		
Remedial action: Ensure that all expected peer MEPs are configured correctly.		

Table 3-377 MepMmg

Alarm	Attributes	Applicable major release
Name: MepMmg (3728) Type: oamAlarm Package: ethernetoam.MepMmg Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mmg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives a CCM frame with correct MEG level but incorrect MEG ID.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with correct MEG level but incorrect MEG ID.		

Table 3-378 MepXcon

Alarm	Attributes	Applicable major release
Name: MepXcon (5510) Type: oamAlarm Package: ethernetoam.MepXcon Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MepXcon	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when MEP Cross Connect CCM is detected.		
Remedial action: Ensure that all expected peer MEPs are configured correctly.		

Table 3-379 MismatchFiber

Alarm	Attributes	Applicable major release
Name: MismatchFiber (3374) Type: communicationsAlarm Package: equipment.MismatchFiber Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MismatchFiber	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Fiber connection mismatch is detected.		
Remedial action: This alarm is raised when a mismatch in the add channel count between the LD card and its assigned WTOCM port is detected. Please check the fibering between LD and WTOCM pack, make sure the fibering matches the WTOCM port provisioning.		

Table 3-380 MissingWaveKey

Alarm	Attributes	Applicable major release
Name: MissingWaveKey (4512) Type: communicationsAlarm Package: equipment.MissingWaveKey Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los Applicable probable causes: • Los • UsLos • LosOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel absent is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-381 MixedPFUsed

Alarm	Attributes	Applicable major release
Name: MixedPFUsed (3376) Type: equipmentAlarm Package: equipment.MixedPFUsed Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MixedPFUsed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Mixed types of power filters used is detected.		
Remedial action: This alarm indicates that two different types of power filters are provisioned in the shelf. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Identify the power filter model engineered for the installation.\n 2. Equip the correct matching power filters.\n 3. Ensure the two power filters are the same type.		

Table 3-382 MJCPF

Alarm	Attributes	Applicable major release
Name: MJCPF (9609) Type: equipmentAlarm Package: equipment.MJCPF Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MJCPF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OT major circuit pack failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-383 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 3-384 ModulatorOutputPowerOutOfRange

Alarm	Attributes	Applicable major release
Name: ModulatorOutputPowerOutOfRange (2051) Type: equipmentAlarm Package: equipment. ModulatorOutputPowerOutOfRange Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ModOutOOR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-384 ModulatorOutputPowerOutOfRange (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Modulator output power out of range is detected.		
Remedial action: This procedure details the corrective action for an MODOUTOOR against the OT port. At the end of each step wait to see if the fault clears. If not, continue with the next step.1. If another card failure is reported on the card, follow the procedure for that specific alarm.2. If the port is pluggable module, remove and reinsert the same module. If the alarm does not clear, replace the module.		

Table 3-385 Msim

Alarm	Attributes	Applicable major release
Name: Msim (3377) Type: communicationsAlarm Package: equipment.Msim Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Msim	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Multiplex Structure Identifier Mismatch is detected.		
Remedial action: Please follow the below steps to clear this alarm:\n 1. Check if there is a signal degraded alarm reported at OT Port. Perform the corrective action for clearing the alarms found.\n 2. After all degraded alarms are cleared retrieve the Digital Wrapper performance monitoring group by executing the following command on node CLI: "show interface card_type shelf slot L1 PM DW".\n 3. Check whether uncorrectable FEC bit errors are reported. If so, perform the action for clearing the signal degraded alarms.\n 4. After all signal degraded alarms are cleared and no uncorrectable bit errors are reported, check whether the input OTU signal MSI byte is compliant with received OT card settings.		

Table 3-386 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 3-387 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 3-387 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 3-388 NEModeMismatch

Alarm	Attributes	Applicable major release
Name: NEModeMismatch (3963) Type: equipmentAlarm Package: equipment.NEModeMismatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NEModeMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when NE Mode Mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-389 NeNotReachable

Alarm	Attributes	Applicable major release
Name: NeNotReachable (8231) Type: equipmentAlarm Package: gmpls.NeNotReachable Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeNotReachable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication between the GMRE and the managed NE is disturbed.		
Remedial action: Not Available.		

Table 3-390 NetworkTimingProtocolOutOfSync

Alarm	Attributes	Applicable major release
Name: NetworkTimingProtocolOutOfSync (4865) Type: communicationsAlarm Package: netw.NetworkTimingProtocolOutOfSync Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NtpOoSync	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when NTP is enabled but not in sync with NTP server is detected.		

Table 3-390 NetworkTimingProtocolOutOfSync (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Verify provisioned servers are valid and reachable. If not, consult network engineering for correct server addresses. 2. Perform a warm reset on the Equipment Controller that is raising the NTPOOSYNC condition.3. Perform a cold reset on the Equipment Controller that is raising the NTPOOSYNC condition.4. Reseat the Equipment Controller that is raising the NTPOOSYNC condition.5. Replace the Equipment Controller that is raising the NTPOOSYNC condition. Follow the return and repair process to return the card to an authorized repair center for replacement.		

Table 3-391 NeUnreachable

Alarm	Attributes	Applicable major release
Name: NeUnreachable (5575) Type: communicationsAlarm Package: netw.NeUnreachable Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeUnreachable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when NE not reachable.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-392 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 3-393 NKM

Alarm	Attributes	Applicable major release
Name: NKM (3964) Type: communicationsAlarm Package: equipment.NKM Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NKM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Encryption Next Key Mismatch is detected.		

Table 3-393 NKM (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to node Troubleshooting guide for detailed steps for corrective action.		

Table 3-394 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 3-395 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 3-396 NodeDeg

Alarm	Attributes	Applicable major release
Name: NodeDeg (5576) Type: communicationsAlarm Package: netw.NodeDeg Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeDeg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE degraded.		

Table 3-396 NodeDeg (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-397 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 3-398 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 3-399 NoDeviceFound

Alarm	Attributes	Applicable major release
Name: NoDeviceFound (4962) Type: equipmentAlarm Package: rmd.NoDeviceFound Raised on class: rmd.Device	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdNDF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the RMD Device can not be found.		

Table 3-399 NoDeviceFound (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - Please ensure the RMD is installed correctly.		

Table 3-400 NominalUnavailableCommunicationProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableCommunicationProblem (8232) Type: communicationsAlarm Package: gmpls. NominalUnavailableCommunicationProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableCommunicationProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed due to control plane problem.		
Remedial action: Not Available.		

Table 3-401 NominalUnavailableConfigurationProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableConfigurationProblem (8233) Type: communicationsAlarm Package: gmpls. NominalUnavailableConfigurationProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableConfigurationProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route is not active due to a wrong configuration (could be either node, link or label).		
Remedial action: Not Available.		

Table 3-402 NominalUnavailableIndeterminateProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableIndeterminateProblem (8234) Type: communicationsAlarm Package: gmpls. NominalUnavailableIndeterminateProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableIndeterminateProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed for no specific reason.		
Remedial action: Not Available.		

Table 3-403 NominalUnavailableReversionPreempt

Alarm	Attributes	Applicable major release
Name: NominalUnavailableReversionPreempt (8235) Type: communicationsAlarm Package: gmpls.NominalUnavailableReversionPreempt Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableReversionPreempt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route is not active due to a resource currently being used by a lower priority LSP.		
Remedial action: Not Available.		

Table 3-404 NominalUnavailableTransmissionProblem

Alarm	Attributes	Applicable major release
Name: NominalUnavailableTransmissionProblem (8237) Type: communicationsAlarm Package: gmpls.NominalUnavailableTransmissionProblem Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalUnavailableTransmissionProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal route failed due to data plane problem.		
Remedial action: Not Available.		

Table 3-405 NotAllowPowered

Alarm	Attributes	Applicable major release
Name: NotAllowPowered (8439) Type: equipmentAlarm Package: equipment.NotAllowPowered Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NotAllowPowered	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Card not allowed powered		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-406 NoTdmPayload

Alarm	Attributes	Applicable major release
Name: NoTdmPayload (5595) Type: communicationsAlarm Package: rmd.NoTdmPayload Raised on class: rmd.TsopChannel	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdTsopNoTdmPl	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when 8 contiguous TSoP packets received with L-bit =" 1. It means that the far end is experiencing a TDM LOS or LOF condition."		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-407 NtpChkSig

Alarm	Attributes	Applicable major release
Name: NtpChkSig (5403) Type: communicationsAlarm Package: netw.NtpChkSig Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NtpAuthFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid signatures are discovered on incoming NTP packets.		
Remedial action: Verify that the authentication signatures are valid for the NTP server.		

Table 3-408 NtpLor

Alarm	Attributes	Applicable major release
Name: NtpLor (3888) Type: equipmentAlarm Package: netw.NtpLor Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NtpLor	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Multiple references provisioned backup not available is detected.		

Table 3-408 NtpLor (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify provisioned servers are valid and reachable. If not, consult network engineering for correct server addresses.Perform a warm reset on the Equipment Controller that is raising the NTPOOSYNC condition.Perform a cold reset on the Equipment Controller that is raising the NTPOOSYNC condition.Reseat the Equipment Controller that is raising the NTPOOSYNC condition.Replace the Equipment Controller that is raising the NTPOOSYNC condition. Follow the return and repair process to return the card to an authorized repair center for replacement.		

Table 3-409 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 3-410 NunvComm

Alarm	Attributes	Applicable major release
Name: NunvComm (5577) Type: communicationsAlarm Package: netw.NunvComm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvComm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - communication problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-411 NunvConfig

Alarm	Attributes	Applicable major release
Name: NunvConfig (5578) Type: communicationsAlarm Package: netw.NunvConfig Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvConfig	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - configuration problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-412 NunvIndetermined

Alarm	Attributes	Applicable major release
Name: NunvIndetermined (5579) Type: communicationsAlarm Package: netw.NunvIndetermined Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvIndetermined	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - indetermined problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-413 NunvReversion

Alarm	Attributes	Applicable major release
Name: NunvReversion (5580) Type: communicationsAlarm Package: netw.NunvReversion Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvReversion	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - reversion preempt.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-414 NunvTpBlocked

Alarm	Attributes	Applicable major release
Name: NunvTpBlocked (5581) Type: communicationsAlarm Package: netw.NunvTpBlocked Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvTpBlocked	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - TP blocked.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-415 NunvTransmission

Alarm	Attributes	Applicable major release
Name: NunvTransmission (5582) Type: communicationsAlarm Package: netw.NunvTransmission Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NunvTransmission	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal unavailable - transmission problem.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-416 NvMismatch

Alarm	Attributes	Applicable major release
Name: NvMismatch (5583) Type: communicationsAlarm Package: netw.NvMismatch Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NvMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when DPR NV mismatch.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-417 OAPumpLaserBiasCurrentHigh

Alarm	Attributes	Applicable major release
Name: OAPumpLaserBiasCurrentHigh (4513) Type: equipmentAlarm Package: equipment.OAPumpLaserBiasCurrentHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpBiasCurrHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser bias current high is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-418 OAPumpLaserBiasCurrentHighC

Alarm	Attributes	Applicable major release
Name: OAPumpLaserBiasCurrentHighC (11102) Type: equipmentAlarm Package: equipment.OAPumpLaserBiasCurrentHighC Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpBiasCurrHighC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser bias current high C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-419 OAPumpLaserBiasCurrentHighL

Alarm	Attributes	Applicable major release
Name: OAPumpLaserBiasCurrentHighL (11103) Type: equipmentAlarm Package: equipment.OAPumpLaserBiasCurrentHighL Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpBiasCurrHighL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser bias current high L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-420 OAPumpLaserTempHigh

Alarm	Attributes	Applicable major release
Name: OAPumpLaserTempHigh (4514) Type: equipmentAlarm Package: equipment.OAPumpLaserTempHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpTempHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser temperature high is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-421 OAPumpLaserTempHighC

Alarm	Attributes	Applicable major release
Name: OAPumpLaserTempHighC (11104) Type: equipmentAlarm Package: equipment.OAPumpLaserTempHighC Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpTempHighC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser temperature high C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-422 OAPumpLaserTempHighL

Alarm	Attributes	Applicable major release
Name: OAPumpLaserTempHighL (11105) Type: equipmentAlarm Package: equipment.OAPumpLaserTempHighL Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OaPumpTempHighL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OA pump laser temperature high L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-423 OCCPCR

Alarm	Attributes	Applicable major release
Name: OCCPCR (9641) Type: equipmentAlarm Package: equipment.OCCPCR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OCCPCR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optics Controller Coherent, Port Critical .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-424 OCCPMJ

Alarm	Attributes	Applicable major release
Name: OCCPMJ (9642) Type: equipmentAlarm Package: equipment.OCCPMJ Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OCCPMJ	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optics Controller Coherent, Port Major .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-425 OCCPMN

Alarm	Attributes	Applicable major release
Name: OCCPMN (9643) Type: equipmentAlarm Package: equipment.OCCPMN Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OCCPMN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optics Controller Coherent, Port Minor .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-426 OchFdi

Alarm	Attributes	Applicable major release
Name: OchFdi (4516) Type: communicationsAlarm Package: equipment.OchFdi Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchFdi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel FDI is detected.		
Remedial action: An automatic and fully distributed capability which indicates a failure in a server networking layer (e.g., Physical Layer). When used with other mechanisms such as CV (Connectivity Verification), it can indicate defects such as misbranching of LSPs and errors in swapping LSP label.Please refer relevant section in 1830 Troubleshooting guide for either OCHFDI (Optical Channel Forward Defect Indication) or VTSFDI (VTS Forward Defect Indication)		

Table 3-427 OchKeysReused

Alarm	Attributes	Applicable major release
Name: OchKeysReused (5180) Type: communicationsAlarm Package: equipment.OchKeysReused Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchKeysReused	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Wave Key pair is re-used for channel on Node.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-428 OchKeyUnavail

Alarm	Attributes	Applicable major release
Name: OchKeyUnavail (5179) Type: communicationsAlarm Package: equipment.OchKeyUnavail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchKeyUnavail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Wave Key is Not Available.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-429 OchLos

Alarm	Attributes	Applicable major release
Name: OchLos (4517) Type: communicationsAlarm Package: equipment.OchLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los Applicable probable causes: • Los • LosP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal - OCH is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-430 OchPdi

Alarm	Attributes	Applicable major release
Name: OchPdi (4518) Type: communicationsAlarm Package: equipment.OchPdi Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchPdi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel PDI is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-431 OciOut

Alarm	Attributes	Applicable major release
Name: OciOut (4519) Type: communicationsAlarm Package: equipment.OciOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OciOut Applicable probable causes: • OciOut • OCI	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Open Connection Indication - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-432 OcsUnavail

Alarm	Attributes	Applicable major release
Name: OcsUnavail (4384) Type: communicationsAlarm Package: netw.OcsUnavail Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OcsUnavail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when DWDM-OCS link down is detected.		
Remedial action: Proceed to Procedure - Clear DWDM-OCS link down in 1830 Troubleshooting guide.		

Table 3-433 OduAis

Alarm	Attributes	Applicable major release
Name: OduAis (3379) Type: communicationsAlarm Package: equipment.OduAis Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OduAis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU-AIS is detected.		

Table 3-433 OduAis (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that the OT port has detected an ODU-AIS at the ODUk level. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Retrieve power level reading on the local OT port.\n 2. If power level is low on the DWDM facing port, identify the associated OCh trail and verify the power levels along the OCh trail.\n 3. Identify the farthest upstream point relative to the far end OTUk port at which power level falls within the expected range.\n 4. Check the alarms/conditions on the node located in step 3 or the node immediately upstream from point identified in step 3.\n 5. Correct the problem identified in Step 4.\n 6. If all the power levels along the OCh trails fall within the target range, locate the fiber connected directly to receiver of the port which detects SSF condition.\n 7. Clean the fiber.\n 8. Replace the fiber.\n 9. If the problem is detected on the client port of 11STAR1 OT, and the power level is within the operating range, check for pluggable module alarms.\n 10. Replace the pluggable module.		

Table 3-434 OduAisEgress

Alarm	Attributes	Applicable major release
Name: OduAisEgress (3380) Type: communicationsAlarm Package: equipment.OduAisEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OduAisEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU Egress - AIS is detected.		
Remedial action: 1. Retrieve power level reading on the local OT port. 2. If power level is low on the DWDM facing port, identify the associated OCh trail and verify the power levels along the OCh trail.3. Identify the farthest upstream point relative to the far end OTUk port at which power level falls within the expected range. 4. Check the alarms/conditions on the node located in Step 3 or the node immediately upstream from point identified in Step 3.5. Correct the problem identified in Step 4.6. If all power levels along the OCh trails fall within the target range, locate the fiber connected directly to receiver of the port which detects SSFODUEGR condition. 7. Clean the fiber.8. If cleaning the fiber does not clear the problem, replace the fiber.9. If the problem is detected on the client port of OT, and the power level is within the operating range, check for pluggable module alarms. 10. Replace the pluggable module.		

Table 3-435 OduAisOut

Alarm	Attributes	Applicable major release
Name: OduAisOut (4520) Type: communicationsAlarm Package: equipment.OduAisOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OduAisOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ODU-AIS OUT is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-436 OmsSSF

Alarm	Attributes	Applicable major release
Name: OmsSSF (3965) Type: communicationsAlarm Package: equipment.OmsSSF Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OmsSSF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OMS Server Signal Failure is detected.		
Remedial action: 1 Check the alarms/conditions for the ingress transmission defects which has been report on the same LD point for OMS Server Signal Failure.2 Identify the OTS layer alarm/condition (such as LOS-P) relative to SSF-OMS.3 Perform the steps in Procedure : Clear Incoming payload LOS for clearing the identified alarm/condition.4 Refresh the list of current alarms, and check whether the OMS SSF alarm has cleared.		

Table 3-437 OneTimingModuleFailed

Alarm	Attributes	Applicable major release
Name: OneTimingModuleFailed (4521) Type: equipmentAlarm Package: equipment.OneTimingModuleFailed Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncClk	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing synchronization unit failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-438 OpenConnectionIndication

Alarm	Attributes	Applicable major release
Name: OpenConnectionIndication (4522) Type: communicationsAlarm Package: equipment.OpenConnectionIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Oci Applicable probable causes: • Oci • OpenConnectionIndicationEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Open Connection Indication is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-439 OpenConnectionIndicationEgress

Alarm	Attributes	Applicable major release
Name: OpenConnectionIndicationEgress (4923) Type: communicationsAlarm Package: equipment.OpenConnectionIndicationEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpenConnectionIndication-Egress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Open Connection Indication Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-440 OprPwrHigh

Alarm	Attributes	Applicable major release
Name: OprPwrHigh (3381) Type: communicationsAlarm Package: equipment.OprPwrHigh Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too high is detected.		
Remedial action: This alarm is raised when the signal power into the LINE or SIG port of an amplifier is too high. For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-441 OprPwrHighC

Alarm	Attributes	Applicable major release
Name: OprPwrHighC (11112) Type: communicationsAlarm Package: equipment.OprPwrHighC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrHighC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too high C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-442 OprPwrHighL

Alarm	Attributes	Applicable major release
Name: OprPwrHighL (11113) Type: communicationsAlarm Package: equipment.OprPwrHighL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrHighL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too high L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-443 OprPwrLow

Alarm	Attributes	Applicable major release
Name: OprPwrLow (3382) Type: communicationsAlarm Package: equipment.OprPwrLow Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too low is detected.		
Remedial action: This alarm is raised when the signal power into the LINE or SIG port of an amplifier is too low. For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-444 OprPwrLowC

Alarm	Attributes	Applicable major release
Name: OprPwrLowC (11114) Type: communicationsAlarm Package: equipment.OprPwrLowC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrLowC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too low C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-445 OprPwrLowL

Alarm	Attributes	Applicable major release
Name: OprPwrLowL (11115) Type: communicationsAlarm Package: equipment.OprPwrLowL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprPwrLowL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Out of operational range - input power too low L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-446 OprTx

Alarm	Attributes	Applicable major release
Name: OprTx (3383) Type: communicationsAlarm Package: equipment.OprTx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprTx	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel power unstable is detected.		
Remedial action: This alarm is raised on cards with a Wavelength Tracker detect point when the power is outside of the provisioned power range. For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-447 OpticalFeasibilityViolation

Alarm	Attributes	Applicable major release
Name: OpticalFeasibilityViolation (9629) Type: communicationsAlarm Package: gmpls.OpticalFeasibilityViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpticalFeasibilityViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when nominal route of the LSP breaks the constraints of optical feasibility calculated by the path computation.		
Remedial action: Not Available.		

Table 3-448 OpticalOutputPowerUnachievable

Alarm	Attributes	Applicable major release
Name: OpticalOutputPowerUnachievable (4524) Type: communicationsAlarm Package: equipment. OpticalOutputPowerUnachievable Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprUnachieve	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel power unachievable is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-449 OpticalParamErr

Alarm	Attributes	Applicable major release
Name: OpticalParamErr (5584) Type: communicationsAlarm Package: netw.OpticalParamErr Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpticalParamErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when optical parameter file error.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-450 OpticalParameterFileError

Alarm	Attributes	Applicable major release
Name: OpticalParameterFileError (8238) Type: equipmentAlarm Package: gmpls.OpticalParameterFileError Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpticalParameterFileError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the last downloaded file with optical feasibility target values (from the EPT) is not valid.		
Remedial action: Not Available.		

Table 3-451 OpticalPowerDeviation

Alarm	Attributes	Applicable major release
Name: OpticalPowerDeviation (4525) Type: communicationsAlarm Package: equipment.OpticalPowerDeviation Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Opr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel power unstable is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-452 OpticalPowerReceivedOutOfRange

Alarm	Attributes	Applicable major release
Name: OpticalPowerReceivedOutOfRange (2064) Type: communicationsAlarm Package: equipment. OpticalPowerReceivedOutOfRange Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprOOR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical power received out of range is detected.		

Table 3-452 OpticalPowerReceivedOutOfRange (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that the OT port has detected a received optical power out of range at OCH Layer. Please follow the below steps to clear this alarm:\n 1. Retrieve power level reading on the local port.\n 2. If input power level is lower or higher than required on the port, identify the associated OCh trail and verify the power levels along the OCh trail. If power levels along the upstream OCh trail are outside of their targeted range, then troubleshoot the port before continuing. If any power deviations raise additional alarms, troubleshoot them first.\n 3. If all power levels along the OCh trails fall within the target range, locate the fiber connected directly to receiver of the port.\n 4. Clean the fiber and check it for kinks.\n 5. If step 3 does not clear the alarm, replace the fiber.\n 6. Clean the input port of the OT. If the port is pluggable module, replace the module.		

Table 3-453 OpticalTest

Alarm	Attributes	Applicable major release
Name: OpticalTest (8164) Type: communicationsAlarm Package: equipment.OpticalTest Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OpticalTest	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical testing in progress.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-454 OpticsModuleMismatch

Alarm	Attributes	Applicable major release
Name: OpticsModuleMismatch (2065) Type: equipmentAlarm Package: equipment.OpticsModuleMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MismatchSfpXfp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module mismatch is detected.		
Remedial action: This alarm indicates that either the detected shelf identifier does not match the provisioned shelf identifier, or a pluggable module is installed on an Egress LD. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Verify the type of pluggable module that is currently installed into the alarmed card.\n 2. If the inserted pluggable module is of correct type by the service record but the MODULETYPE attribute is not correct, then modify the MODULETYPE value.\n 3. If the inserted pluggable module is of the incorrect type, then remove the module and insert one that matches the expected module type.\n 4. If the inserted pluggable module is of the correct type, then remove the module and reseat it back into the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-455 OpticsModuleUnknown

Alarm	Attributes	Applicable major release
Name: OpticsModuleUnknown (3386) Type: equipmentAlarm Package: equipment.OpticsModuleUnknown Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnknownSfpXfp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-455 OpticsModuleUnknown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Pluggable Module unknown is detected.		
Remedial action: This alarm indicates that the optics module(pluggable module) inserted in the port is of type that is not recognized and the system cannot obtain manufacturing information of the unit. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. To clear the pack while it is still in service, do one of the following:\n a. Change the notification from a standing alarm to a transient condition, or\n b. Change the MODULETYPE provisioning(from "auto" to "user").\n 2. Perform a warm reset of the card.\n 3. Remove the pluggable module and examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage.\n 4. Remove and replace the pluggable module with another unit of the same type.\n 5. Perform a cold reset of the card.\n 6. Reseat the card.\n 7. If there is no transmission, check that the provisioned signal rate is supported by the pluggable module.\n 8. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-456 OptIntBase

Alarm	Attributes	Applicable major release
Name: OptIntBase (4523) Type: communicationsAlarm Package: equipment.OptIntBase Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OptIntBase	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical Intrusion - Baseline Needed is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-457 OptIntDet

Alarm	Attributes	Applicable major release
Name: OptIntDet (3384) Type: communicationsAlarm Package: equipment.OptIntDet Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OptIntDet	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical Intrusion - Detected is detected.		
Remedial action: Click the Optical Intrusion tab.Select the Clear Optical Intrusion Detected Alarm field, and click Submit.		

Table 3-458 OptIntSusp

Alarm	Attributes	Applicable major release
Name: OptIntSusp (3385) Type: communicationsAlarm Package: equipment.OptIntSusp Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OptIntSusp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Optical Intrusion - Monitoring Suspended is detected.		
Remedial action: Optical intrusion monitoring to the line fibre is suspended due to local or upstream NE conditions. The alarm could be due to a variety of NE alarms such as NET, LOS-P, APR and CARDINIT. The OPTINTSUSP alarm clears when the underlying cause clears.Follow the respective procedure to clear the underlying cause alarms.		

Table 3-459 OSNRMESC

Alarm	Attributes	Applicable major release
Name: OSNRMESC (4922) Type: configurationAlarm Package: equipment.OSNRMESC Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OSNRMESC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OSNR Measurement Exclusive on Selected Channels .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-460 OSPFADJ

Alarm	Attributes	Applicable major release
Name: OSPFADJ (3378) Type: equipmentAlarm Package: equipment.OSPFADJ Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OSPFADJ	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OSPF Adjacency not Full is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-461 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 3-462 OTMCPF

Alarm	Attributes	Applicable major release
Name: OTMCPF (4515) Type: equipmentAlarm Package: equipment.OTMCPF Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OTMCPF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-462 OTMCPF (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when OT minor circuit pack failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-463 OtuAis

Alarm	Attributes	Applicable major release
Name: OtuAis (4526) Type: communicationsAlarm Package: equipment.OtuAis Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OtuAis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OTU AIS is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-464 OutBandCommDegraded

Alarm	Attributes	Applicable major release
Name: OutBandCommDegraded (8239) Type: communicationsAlarm Package: gmpls.OutBandCommDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OutBandCommDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a problem on at least one out-of-band tunnel.		
Remedial action: Not Available.		

Table 3-465 OutBandCommDown

Alarm	Attributes	Applicable major release
Name: OutBandCommDown (8240) Type: communicationsAlarm Package: gmpls.OutBandCommDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OutBandCommDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP communication via the out-of-band tunnel is not working.		
Remedial action: Not Available.		

Table 3-466 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 3-467 PacketCardInit

Alarm	Attributes	Applicable major release
Name: PacketCardInit (8165) Type: equipmentAlarm Package: equipment.PacketCardInit Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PacketCardInit	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Packet card initializing.		

Table 3-467 PacketCardInit (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-468 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 3-469 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 3-470 PayloadTypeMismatch

Alarm	Attributes	Applicable major release
Name: PayloadTypeMismatch (4527) Type: communicationsAlarm Package: equipment.PayloadTypeMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Plm Applicable probable causes: • Plm • PayloadTypeMismatchEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Payload Type Mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-471 PayloadTypeMismatchEgress

Alarm	Attributes	Applicable major release
Name: PayloadTypeMismatchEgress (4924) Type: communicationsAlarm Package: equipment.PayloadTypeMismatchEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PayloadTypeMismatchEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Payload Type Mismatch Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-472 PCSGeneratorActive

Alarm	Attributes	Applicable major release
Name: PCSGeneratorActive (3387) Type: equipmentAlarm Package: equipment.PCSGeneratorActive Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PCSGeneratorActive	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when PCS Generator active is detected.		
Remedial action: This alarm is raised when the signal loopback test is in progress at the 100GA/D client port. To clear this alarm please execute the following command from the node CLI: "config interface card_type shelf slot c1 loopback testsignal disabled".		

Table 3-473 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 3-474 PhysicalLinkPortsMisconfigured

Alarm	Attributes	Applicable major release
Name: PhysicalLinkPortsMisconfigured (239) Type: configurationAlarm Package: netw.PhysicalLinkPortsMisconfigured Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: physicalLinkPortsMisconfig-ured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is an MTU size mismatch between a link endpoint and a port. The alarm clears when the MTUs match.		
Raising condition: ('physicalLinkMisconfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The MTU value(s) on the link endpoint and port must be changed such that they match.		

Table 3-475 PlmOduOut

Alarm	Attributes	Applicable major release
Name: PlmOduOut (4528) Type: communicationsAlarm Package: equipment.PlmOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PlmOduOut Applicable probable causes: • PlmOduOut • PLMP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Payload Mismatch Indication - ODU is detected.		

Table 3-475 PlmOduOut (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-476 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 3-477 PortDegrade

Alarm	Attributes	Applicable major release
Name: PortDegrade (4529) Type: equipmentAlarm Package: equipment.PortDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FacTermDgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port degrade device is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-478 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol- dExceededAlarm	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 3-479 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 3-480 PortFailure

Alarm	Attributes	Applicable major release
Name: PortFailure (2070) Type: equipmentAlarm Package: equipment.PortFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FacTermDev Applicable probable causes: • FacTermDev • Eqpt • Mtcssurv	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module SEEP failure is detected.		
Remedial action: This alarm indicates a port indicates a port initialization failure on the network ports(10G ports). Please follow the below steps to clear this alarm:\n 1. Perform a warm reset of the card.\n 2. Perform a cold reset of the card.\n 3. Reseat the card.\n 4. Remove the pluggable module from the port. Examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage.\n 5. Remove and replace the pluggable module with another unit of the same type.\n 6. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-481 PortMismatch

Alarm	Attributes	Applicable major release
Name: PortMismatch (4530) Type: equipmentAlarm Package: equipment.PortMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port provisioning mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-482 PortTransmissionDegrade

Alarm	Attributes	Applicable major release
Name: PortTransmissionDegrade (2071) Type: equipmentAlarm Package: equipment.PortTransmissionDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LsrOutDgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port transmit degrade is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed corrective action.		

Table 3-483 PortTransmissionFailure

Alarm	Attributes	Applicable major release
Name: PortTransmissionFailure (3388) Type: equipmentAlarm Package: equipment.PortTransmissionFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Trmt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port transmit failure is detected.		
Remedial action: 1. Perform a warm reset of the card.2. Remove the pluggable module from the port on the card it is inserted in. Examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage. If no damage is seen, reinsert the pluggable module into its port.3. Remove and replace the pluggable module with another unit of the same type.4. Perform a cold reset of the card on the card where the pluggable module failure is raised.5. Reseat the card. 6. Replace the card.		

Table 3-484 PowerAdjustFailed

Alarm	Attributes	Applicable major release
Name: PowerAdjustFailed (4531) Type: equipmentAlarm Package: equipment.PowerAdjustFailed Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrAdjFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Adjustment Failure is detected.		

Table 3-484 PowerAdjustFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-485 PowerAdjustLossMarginExceeded

Alarm	Attributes	Applicable major release
Name: PowerAdjustLossMarginExceeded (4532) Type: communicationsAlarm Package: equipment. PowerAdjustLossMarginExceeded Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrMargin	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Adjustment Margin Exceeded is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-486 PowerAdjustRequired

Alarm	Attributes	Applicable major release
Name: PowerAdjustRequired (4533) Type: equipmentAlarm Package: equipment.PowerAdjustRequired Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrAdjReq	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Adjustment Required is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-487 PowerFail

Alarm	Attributes	Applicable major release
Name: PowerFail (4963) Type: equipmentAlarm Package: rmd.PowerFail Raised on class: rmd.Device	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdPWR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is a power failure on the RMD Device.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-488 PowerMgmtSuspended

Alarm	Attributes	Applicable major release
Name: PowerMgmtSuspended (4534) Type: communicationsAlarm Package: equipment.PowerMgmtSuspended Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrSusp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power management suspended is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-489 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-490 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-491 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		

Table 3-491 PowerSupplyFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-492 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-493 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 3-494 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Generated when one of the chassis's power output fails.		

Table 3-494 PowerSupplyOutputFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-495 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-496 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 3-497 PPSLos

Alarm	Attributes	Applicable major release
Name: PPSLos (3966) Type: communicationsAlarm Package: ptp.PPSLos Raised on class: ptp.PTPTOD	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PPSLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of 1PPS Signal is detected.		

Table 3-497 PPSLos (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-498 PrcdrErrTopoOut

Alarm	Attributes	Applicable major release
Name: PrcdrErrTopoOut (3733) Type: equipmentAlarm Package: equipment.PrcdrErrTopoOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrcdrErrTopoOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power management topology invalid-out is detected.		
Remedial action: Valid cross-connects must terminate on one of the following end-points:\n 1. a port marked as "External".\n 2. a port marked as "No-Connect".\n 3. a transponder network port. Please follow the below steps to clear this alarm:\n 1. Examine the cross-connects on the NE, and look for cross-connects that do not conform to the rules.\n 2. Delete the invalid connections. Any service that is running over an invalid cross-connect that is deleted is interrupted.\n 3. Recreate valid cross-connects for the interrupted services.		

Table 3-499 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 3-500 ProtSwitchDeviceFailure

Alarm	Attributes	Applicable major release
Name: ProtSwitchDeviceFailure (4535) Type: equipmentAlarm Package: equipment.ProtSwitchDeviceFailure Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwEqpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Protection switching equipment failure is detected.		

Table 3-500 ProtSwitchDeviceFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-501 PTPFreeRun

Alarm	Attributes	Applicable major release
Name: PTPFreeRun (4953) Type: communicationsAlarm Package: ptp.PTPFreeRun Raised on class: ptp.IEEEPTPClock	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPFreeRun	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when PTP clock in the free-running status .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-502 PTPRefLoss

Alarm	Attributes	Applicable major release
Name: PTPRefLoss (4954) Type: communicationsAlarm Package: ptp.PTPRefLoss Raised on class: ptp.IEEEPTPClock	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPRefLoss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when No available time references .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-503 PTPRefUnstable

Alarm	Attributes	Applicable major release
Name: PTPRefUnstable (4955) Type: communicationsAlarm Package: ptp.PTPRefUnstable Raised on class: ptp.IEEEPTPPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPRefUnstable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when The current time reference is unstable .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-504 PwrAdjComms

Alarm	Attributes	Applicable major release
Name: PwrAdjComms (3734) Type: communicationsAlarm Package: equipment.PwrAdjComms Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrAdjComms	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Inter NE communication timeout blocking power adjustment is detected.		
Remedial action: Please follow following steps to clear this alarm.1. If the PWRADJFAIL alarm occurs with the PWRADJCOMMS alarm, proceed to PWRADJFAIL before continuing with this procedure.2. If the upstream NE is undergoing discovery by an NMS system, wait for the NMS to finish discovery.3.Verify that the topology is set up properly to the upstream NE.4. Verify the local NE can communicate with the upstream NE.5. Repeat Step-3.6.Verify that the upstream NE is functioning as it should. Ensure that there is CN/OSPF connectivity at the NE raising the alarm by checking any other alarms on the NE CN links. Check that the OSC channel is operational.7.Activate an ingress adjust.8. If the ingress adjustment fails, troubleshoot why it failed using the Adjust Result and go to the troubleshooting steps for the PWRADJFAIL alarm.		

Table 3-505 PWRADJFAILADD

Alarm	Attributes	Applicable major release
Name: PWRADJFAILADD (3729) Type: communicationsAlarm Package: equipment.PWRADJFAILADD Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PWRADJFAILADD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-505 PWRADJFAILADD (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Add Power Adjustment Failure is detected.		
Remedial action: Wait until the APR condition has been cleared.Re-try the adjustment.For Further details,Please refer 1830 PSS Node Maintenance and Troubleshooting guide.		

Table 3-506 PWRADJFAILDRP

Alarm	Attributes	Applicable major release
Name: PWRADJFAILDRP (3730) Type: communicationsAlarm Package: equipment.PWRADJFAILDRP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PWRADJFAILDRP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Drop Power Adjustment Failure is detected.		
Remedial action: Wait until the APR condition has been cleared.Re-try the adjustment.For Further details,Please refer 1830 PSS Node Maintenance and Troubleshooting guide.		

Table 3-507 PWRADJREQADD

Alarm	Attributes	Applicable major release
Name: PWRADJREQADD (3731) Type: communicationsAlarm Package: equipment.PWRADJREQADD Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PWRADJREQADD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Add Power Adjustment Required is detected.		
Remedial action: 1. Perform a power adjust operation at the ingress amplifier card or the ALPHG card that has raised the PWRADJREQ alarm.2. If the adjustment is successful, then the PWRADJREQ alarm will be cleared.Continue with Step 3.If the adjustment fails, then the PWRADJFAIL alarm will appear. Proceed to PWRADJFAIL. 3. Follow the appropriate procedures in the 1830 PSS User Provisioning Guide to validate the set parameters of the network per the Network Plan.		

Table 3-508 PWRADJREQDRP

Alarm	Attributes	Applicable major release
Name: PWRADJREQDRP (3732) Type: communicationsAlarm Package: equipment.PWRADJREQDRP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PWRADJREQDRP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Drop Power Adjustment Required is detected.		

Table 3-508 PWRADJREQDRP (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Perform a power adjust operation at the ingress amplifier card or the ALPHG card that has raised the PWRADJREQ alarm.2. If the adjustment is successful, then the PWRADJREQ alarm will be cleared.Continue with Step 3.If the adjustment fails, then the PWRADJFAIL alarm will appear. Proceed to PWRADJFAIL. 3. Follow the appropriate procedures in the 1830 PSS User Provisioning Guide to validate the set parameters of the network per the Network Plan.		

Table 3-509 PwrEdfaMargin

Alarm	Attributes	Applicable major release
Name: PwrEdfaMargin (4536) Type: communicationsAlarm Package: equipment.PwrEdfaMargin Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrEdfaMargin	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when EDFA input power approaching upper limit is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-510 PwrMaxGain

Alarm	Attributes	Applicable major release
Name: PwrMaxGain (2081) Type: communicationsAlarm Package: equipment.PwrMaxGain Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrMaxGain	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Gain Adjustment Exceeded Max Value is detected.		
Remedial action: This alarm indicates that the loss between the upstream NE line and the alarmed LD line is higher than expected.\n For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-511 PwrMaxGainC

Alarm	Attributes	Applicable major release
Name: PwrMaxGainC (11116) Type: communicationsAlarm Package: equipment.PwrMaxGainC Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrMaxGainC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Gain Adjustment Exceeded Max Value C band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-512 PwrMaxGainL

Alarm	Attributes	Applicable major release
Name: PwrMaxGainL (11117) Type: communicationsAlarm Package: equipment.PwrMaxGainL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrMaxGainL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Gain Adjustment Exceeded Max Value L band .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-513 PwrTiltParams

Alarm	Attributes	Applicable major release
Name: PwrTiltParams (3967) Type: communicationsAlarm Package: equipment.PwrTiltParams Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrTiltParams	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Parameters for amplifier tilt adjustment unconfigured is detected.		
Remedial action: Configure the parameters required for automatic tilt adjustment to non-default values, or disable automatic tilt adjustment for the line.		

Table 3-514 PwrTiltSusp

Alarm	Attributes	Applicable major release
Name: PwrTiltSusp (3389) Type: communicationsAlarm Package: equipment.PwrTiltSusp Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrTiltSusp	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Amplifier Gain Tilt Adjustments Suspended is detected.		
Remedial action: This alarm is raised when:\n 1. The automatic amplifier gain tilt adjustments are suspended, in the direction of transmission, for the optical multiplex section originating at the OADM line because optical channel power measurement for the line is impaired.\n 2. It is caused when the channel exceeds the number of attempts it can use to get power information from the Line Out port.\n For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-515 PwrUnbalance

Alarm	Attributes	Applicable major release
Name: PwrUnbalance (3390) Type: communicationsAlarm Package: equipment.PwrUnbalance Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrUnbalance	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when OPS Power Unbalance in OLP is detected.		

Table 3-515 PwrUnbalance (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the difference of input power at A and B ports on OPSA is more than 2 dB. Please follow the below steps to clear this alarm:\n 1. Check whether ingress LD's gains for working and protection paths have been set correctly according to power budget table.\n 2. Check whether Total Output Powers on ingress LD's SIG out port for working and protection paths are in range.\n 3. If all above steps are correct, verify that the fibers to OPSA A/B in ports are not damaged or dirty,and clean or replace them.		

Table 3-516 PwrUnbalanceOms

Alarm	Attributes	Applicable major release
Name: PwrUnbalanceOms (3391) Type: communicationsAlarm Package: equipment.PwrUnbalanceOms Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PwrUnbalanceOms	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Power Unbalance is detected.		
Remedial action: This alarm is raised when the difference of input power at A and B ports on OPSA is more than 2 dB. Please follow the below steps to clear this alarm:\n 1. Check whether ingress LD's gains for working and protection paths have been set correctly according to power budget table.\n 2. Check whether Total Output Powers on ingress LD's SIG out port for working and protection paths are in range.\n 3. If all above steps are correct, verify that the fibers to OPSA A/B in ports are not damaged or dirty,and clean or replace them.See further details in 1830 Troubleshooting guide.		

Table 3-517 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 3-518 RamanSup

Alarm	Attributes	Applicable major release
Name: RamanSup (4537) Type: communicationsAlarm Package: equipment.RamanSup Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RAMANSUP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Raman Suppress - Line is detected.		

Table 3-518 RamanSup (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-519 RcvrOptProg

Alarm	Attributes	Applicable major release
Name: RcvrOptProg (2083) Type: equipmentAlarm Package: equipment.RcvrOptProg Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RcvrOptProg	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Receiver Optimization in Progress is detected.		
Remedial action: This procedure details the corrective action for a RCVROPTPROG against the Line port.1. Wait approximately 15 minutes for the LOS or LOF alarm to clear.2. Ensure that the administrative state of the port is Admin Up. When it is Up, then toggle the administrative state from UP > DOWN > UP.3. If a faulty43STX4P pack caused the RCVROPTPROG alarm, replace with it a new 43STX4 pack. After replacement, if the condition persists, fiber loopback the line side of the 43STX4 pack.Remove the fiber from the port where the LOS or LOF was raised and measure the optical power.If the RCVROPTPROG condition is still present more than 15 minutes after the LOS or LOF alarm clears, the problem may be with the card.If the problem is on the Line input signal of the pack, check the signal. After a 40G OT card has initialized successfully, the Tunable Dispersion Compensator (TDC) and Delay Line Interferometer (DLI) on the line-side receive path will automatically tune to optimize transmission performance. During the TDC/DLI optimization, the RCVROPTPROG alarm is raised to notify the user that the pack is tuning, and transmission is not yet stable. When the TDC/DLI tuning process is completed, the alarm clears.4. Perform a warm reset of the card.5. Perform a cold reset of the card.6. Reseat and replace the card.		

Table 3-520 RDI (ethernetoam)

Alarm	Attributes	Applicable major release
Name: RDI (806) Type: oamAlarm Package: ethernetoam.RDI Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Rdi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The RDI alarm is raised when a MEP receives a CCM frame with the RDI field set.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with the RDI field set.		

Table 3-521 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		

Table 3-521 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 3-522 ReadyToRevert (netw)

Alarm	Attributes	Applicable major release
Name: ReadyToRevert (5586) Type: communicationsAlarm Package: netw.ReadyToRevert Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReadyToRevert	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ready to revert.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-523 ReadyToRevert (gmpls)

Alarm	Attributes	Applicable major release
Name: ReadyToRevert (5586) Type: communicationsAlarm Package: gmpls.ReadyToRevert Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReadyToRevert	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the nominal resources are available again, and a reversion can be done.		
Remedial action: Not Available.		

Table 3-524 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 3-525 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 3-526 RemoteFailureIndication

Alarm	Attributes	Applicable major release
Name: RemoteFailureIndication (4538) Type: communicationsAlarm Package: equipment.RemoteFailureIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanRfi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Fault is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-527 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 3-528 RemotePacketLost

Alarm	Attributes	Applicable major release
Name: RemotePacketLost (5596) Type: communicationsAlarm Package: rmd.RemotePacketLost Raised on class: rmd.TsopChannel	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdTsopRPL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when 8 contiguous TSoP packets received with R-bit =" 1. Cleared when 8 contiguous TSoP packets received with R-bit = 0."		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-529 ReplUnitMissMOD

Alarm	Attributes	Applicable major release
Name: ReplUnitMissMOD (3392) Type: equipmentAlarm Package: equipment.ReplUnitMissMOD Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplUnitMissMOD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module missing is detected.		
Remedial action: This alarm indicates that the optics module(pluggable module) for the port is missing or the card is not able to successfully detect the presence of the module. Please follow the below steps to clear this alarm:\n 1. If there is no pluggable module in the port where the pluggable module missing condition is raised, then insert one that is appropriate for that transponder card.\n 2. Perform a warm reset of the card.\n 3. Remove the pluggable module from the port on the card it is inserted in. Examine the connector on the SFP and the receptacle connector on the card where the SFP plugs into for any damage. If no damage is seen, then reinsert the pluggable module into its port.\n 4. Remove and replace the pluggable module with another unit of the same type.\n 5. Perform a cold reset of the card.\n 6. Reseat the card.\n 7. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-530 Rerouted

Alarm	Attributes	Applicable major release
Name: Rerouted (8244) Type: communicationsAlarm Package: gmpls.Rerouted Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Rerouted	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-530 Rerouted (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the current route of the LSP is not the nominal route.		
Remedial action: Not Available.		

Table 3-531 ReRouted

Alarm	Attributes	Applicable major release
Name: ReRouted (5585) Type: communicationsAlarm Package: netw.ReRouted Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReRouted	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when rerouted.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-532 RerouteNotPossible

Alarm	Attributes	Applicable major release
Name: RerouteNotPossible (8243) Type: communicationsAlarm Package: gmpls.RerouteNotPossible Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RerouteNotPossible	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when no backup route can be found or activated for the LSP.		
Remedial action: Not Available.		

Table 3-533 RestorationDisabled

Alarm	Attributes	Applicable major release
Name: RestorationDisabled (5587) Type: communicationsAlarm Package: netw.RestorationDisabled Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RestorationDisabled	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GMRE automatic restoration disabled.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-534 RestrictedConnectivity

Alarm	Attributes	Applicable major release
Name: RestrictedConnectivity (8441) Type: equipmentAlarm Package: equipment.RestrictedConnectivity Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RestrictedConnectivity	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Restricted Connectivity due to subnet connectivity loss. Operator action required.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-535 RfiEgress

Alarm	Attributes	Applicable major release
Name: RfiEgress (4539) Type: communicationsAlarm Package: equipment.RfiEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RfiEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Client Remote Fault is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-536 RouteNotPossible

Alarm	Attributes	Applicable major release
Name: RouteNotPossible (5588) Type: communicationsAlarm Package: netw.RouteNotPossible Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RouteNotPossible	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when route not possible.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-537 RSVPDegraded

Alarm	Attributes	Applicable major release
Name: RSVPDegraded (8241) Type: communicationsAlarm Package: gmpls.RSVPDegraded Raised on class: gmpls.CPNode	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RSVPDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the communication to the neighbor node for RSVP traffic is not working.		
Remedial action: Not Available.		

Table 3-538 RSVPDown

Alarm	Attributes	Applicable major release
Name: RSVPDown (8242) Type: communicationsAlarm Package: gmpls.RSVPDown Raised on class: gmpls.CPNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RSVPDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the RSVP communication to the neighbor is down.		
Remedial action: Not Available.		

Table 3-539 SapMacAddrLimitReached

Alarm	Attributes	Applicable major release
Name: SapMacAddrLimitReached (5597) Type: resourceAlarm Package: vpls.SapMacAddrLimitReached Raised on class: vpls.L2AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the number of MAC address entries in the SAP FDB table reaches 75% of the maximum number of FDB Entries		
Remedial action: Informational		

Table 3-540 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 3-541 SC1LinkDegrade

Alarm	Attributes	Applicable major release
Name: SC1LinkDegrade (11118) Type: equipmentAlarm Package: equipment.SC1LinkDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC1LinkDegrade	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link degraded from switch card 1 .		

Table 3-541 SC1LinkDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-542 SC1LinkFail

Alarm	Attributes	Applicable major release
Name: SC1LinkFail (11119) Type: equipmentAlarm Package: equipment.SC1LinkFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC1LinkFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link failure from switch card 1 .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-543 SC2LinkDegrade

Alarm	Attributes	Applicable major release
Name: SC2LinkDegrade (11120) Type: equipmentAlarm Package: equipment.SC2LinkDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC2LinkDegrade	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link degraded from switch card 2 .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-544 SC2LinkFail

Alarm	Attributes	Applicable major release
Name: SC2LinkFail (11121) Type: equipmentAlarm Package: equipment.SC2LinkFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC2LinkFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link failure from switch card 2 .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-545 SC3LinkDegrade

Alarm	Attributes	Applicable major release
Name: SC3LinkDegrade (11122) Type: equipmentAlarm Package: equipment.SC3LinkDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC3LinkDegrade	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link degraded from switch card 3 .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-546 SC3LinkFail

Alarm	Attributes	Applicable major release
Name: SC3LinkFail (11123) Type: equipmentAlarm Package: equipment.SC3LinkFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SC3LinkFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link failure from switch card 3 .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-547 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 3-548 SCLinkDegrade

Alarm	Attributes	Applicable major release
Name: SCLinkDegrade (11124) Type: equipmentAlarm Package: equipment.SCLinkDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SCLinkDegrade	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-548 SCLinkDegrade (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Internal payload link degraded from io card .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-549 SCLinkFail

Alarm	Attributes	Applicable major release
Name: SCLinkFail (11125) Type: equipmentAlarm Package: equipment.SCLinkFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SCLinkFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal payload link failure from io card .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-550 SdhAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SdhAlarmIndicationSignal (4540) Type: communicationsAlarm Package: equipment.SdhAlarmIndicationSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AisL Applicable probable causes: • AisL • AisLM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS Line/MS is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-551 SdhLossOfClock

Alarm	Attributes	Applicable major release
Name: SdhLossOfClock (4541) Type: communicationsAlarm Package: equipment.SdhLossOfClock Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LostClock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-552 SdhLossOfFrame

Alarm	Attributes	Applicable major release
Name: SdhLossOfFrame (4542) Type: communicationsAlarm Package: equipment.SdhLossOfFrame Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-553 SdhLossOfPointer

Alarm	Attributes	Applicable major release
Name: SdhLossOfPointer (4543) Type: communicationsAlarm Package: equipment.SdhLossOfPointer Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LostClock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-554 SdhLossOfSignal

Alarm	Attributes	Applicable major release
Name: SdhLossOfSignal (4544) Type: communicationsAlarm Package: equipment.SdhLossOfSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los Applicable probable causes: • Los • LosP • LosOut • LosLdSig • LanLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of signal is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-555 SdhMultiplexSectionRemoteFailureIndication

Alarm	Attributes	Applicable major release
Name: SdhMultiplexSectionRemoteFailureIndication (4545) Type: communicationsAlarm Package: equipment. SdhMultiplexSectionRemoteFailureIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LanRfi	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Remote Fault is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-556 SdhRegeneratorSectionTraceMismatch

Alarm	Attributes	Applicable major release
Name: SdhRegeneratorSectionTraceMismatch (4546) Type: communicationsAlarm Package: equipment. SdhRegeneratorSectionTraceMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Tim	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trace Identifier Mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-557 SdhSignalDegrade

Alarm	Attributes	Applicable major release
Name: SdhSignalDegrade (4547) Type: communicationsAlarm Package: equipment.SdhSignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Signal Degrade is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-558 SdhSignalFailure

Alarm	Attributes	Applicable major release
Name: SdhSignalFailure (4548) Type: communicationsAlarm Package: equipment.SdhSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Excessive BER is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-559 SDKMismatch

Alarm	Attributes	Applicable major release
Name: SDKMismatch (8442) Type: equipmentAlarm Package: equipment.SDKMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SDKMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: SDK Mismatch.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-560 ServerSignalFailure

Alarm	Attributes	Applicable major release
Name: ServerSignalFailure (4549) Type: communicationsAlarm Package: equipment.ServerSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OscSsf Applicable probable causes: • OscSsf • Ssf • SsfOdu • ServerSignalFailureEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server signal failure - OSC is detected.		
Remedial action: This alarm indicates that the OT port has detected an Optical Channel (Och) Server Signal Failure. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Retrieve power level reading on the local OT port.\n 2. If power level is low on the DWDM facing port, identify the associated OCh trail and verify the power levels along the OCh trail.\n 3. Identify the farthest upstream point relative to the far end OTUk port at which power level falls within the expected range.\n 4. Check the alarms/conditions on the node located in step 3 or the node immediately upstream from point identified in step 3.\n 5. Correct the problem identified in Step 4.\n 6. If all the power levels along the OCh trails fall within the target range, locate the fiber connected directly to receiver of the port which detects SSF condition.\n 7. Clean the fiber.\n 8. Replace the fiber.\n 9. If the problem is detected on the client port of 11STAR1 OT, and the power level is within the operating range, check for pluggable module alarms.\n 10. Replace the pluggable module.		

Table 3-561 ServerSignalFailureEgress

Alarm	Attributes	Applicable major release
Name: ServerSignalFailureEgress (4933) Type: communicationsAlarm Package: equipment.ServerSignalFailureEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ServerSignalFailureEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-562 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		

Table 3-562 ServiceSiteDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 3-563 SfpEOL

Alarm	Attributes	Applicable major release
Name: SfpEOL (4550) Type: communicationsAlarm Package: equipment.SfpEOL Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfpEOL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SFP or XFP Laser end of life is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-564 SFPEquipmentFail

Alarm	Attributes	Applicable major release
Name: SFPEquipmentFail (4964) Type: equipmentAlarm Package: rmd.SFPEquipmentFail Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfEQF	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is an equipment failure on the RMD SFP.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-565 SFPLossOfSignal

Alarm	Attributes	Applicable major release
Name: SFPLossOfSignal (4965) Type: communicationsAlarm Package: rmd.SFPLossOfSignal Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfLOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected. Only applicable to customer ports.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-566 SfpReceiverPwrOOR

Alarm	Attributes	Applicable major release
Name: SfpReceiverPwrOOR (4551) Type: equipmentAlarm Package: equipment.SfpReceiverPwrOOR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfpReceiverPwrOOR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module optical receiver power out of range is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-567 SfpTempOOR

Alarm	Attributes	Applicable major release
Name: SfpTempOOR (2088) Type: communicationsAlarm Package: equipment.SfpTempOOR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfpTempOOR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SFP or XFP laser temperature out of range is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-568 SfpTrmtPwrOOR

Alarm	Attributes	Applicable major release
Name: SfpTrmtPwrOOR (4552) Type: communicationsAlarm Package: equipment.SfpTrmtPwrOOR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfpTrmtPwrOOR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SFP or XFP optical transmit power out of range is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-569 ShelfAirFilterMaintenance

Alarm	Attributes	Applicable major release
Name: ShelfAirFilterMaintenance (11126) Type: equipmentAlarm Package: equipment.ShelfAirFilterMaintenance Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InspectAirFilter	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Inspect Shelf Air Filter.		
Remedial action: Please refer 1830 PSS Troubleshooting guide for detailed steps for corrective action.		

Table 3-570 ShelfIdMismatch

Alarm	Attributes	Applicable major release
Name: ShelfIdMismatch (8443) Type: equipmentAlarm Package: equipment.ShelfIdMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfIdMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Shelf-ID mismatch		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-571 ShelfIncon

Alarm	Attributes	Applicable major release
Name: ShelfIncon (8167) Type: equipmentAlarm Package: equipment.ShelfIncon Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfIncon	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf data inconsistent.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-572 ShelfInventoryError

Alarm	Attributes	Applicable major release
Name: ShelfInventoryError (11127) Type: equipmentAlarm Package: equipment.ShelfInventoryError Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfInvError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf Inventory Error .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-573 ShelfInventoryMismatch

Alarm	Attributes	Applicable major release
Name: ShelfInventoryMismatch (11128) Type: equipmentAlarm Package: equipment.ShelfInventoryMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfInvMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf Inventory Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-574 ShelfInVoltHigh

Alarm	Attributes	Applicable major release
Name: ShelfInVoltHigh (4553) Type: equipmentAlarm Package: equipment.ShelfInVoltHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfInVoltHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf Supply Voltage High is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-575 ShelfInVoltLow

Alarm	Attributes	Applicable major release
Name: ShelfInVoltLow (4554) Type: equipmentAlarm Package: equipment.ShelfInVoltLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfInVoltLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf Supply Voltage Low is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-576 ShelfInVoltMaxCur

Alarm	Attributes	Applicable major release
Name: ShelfInVoltMaxCur (5448) Type: communicationsAlarm Package: equipment.ShelfInVoltMaxCur Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfInVoltMaxCur	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Low input voltage floor defect .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-577 ShelfLoadWarning

Alarm	Attributes	Applicable major release
Name: ShelfLoadWarning (8444) Type: equipmentAlarm Package: equipment.ShelfLoadWarning Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShelfLoadWarning	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Shelf load warning		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-578 ShelfMismatch

Alarm	Attributes	Applicable major release
Name: ShelfMismatch (2090) Type: equipmentAlarm Package: equipment.ShelfMismatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Shelf mismatch is detected.		
Remedial action: This alarm is raised when the detected DCM or SFD44 shelf serial number does not match the provisioned serial number. Please follow the below steps to clear this alarm:\n 1. Review DCM and SFD44 shelf serial numbers and make corrections as needed.\n 2. Display the shelf list.\n 3. View the results, and use the following commands as needed:\n a. To change as DCM/SFD44 shelf serial number("config shelf <shelf> serialnum <string>").\n b. To create a new shelf("config shelf <shelf> type dcm" or "config shelf <shelf> type sfd44").\n c. To delete an existing shelf("config shelf <shelf> type empty").\n 4. If the correct serial number is provisioned, but the wrong DCM or SFD44 module is connected, replace the module with one which has the correct serial number.		

Table 3-579 SignalDegrade

Alarm	Attributes	Applicable major release
Name: SignalDegrade (2091) Type: communicationsAlarm Package: equipment.SignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Deg Applicable probable causes: • Deg • SignalDegradeEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Signal Degrade - ODU is detected.		

Table 3-579 SignalDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-580 SignalDegradeEgress

Alarm	Attributes	Applicable major release
Name: SignalDegradeEgress (4934) Type: communicationsAlarm Package: equipment.SignalDegradeEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalDegradeEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Signal Degrade Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-581 SLCBOOTCONTCOM

Alarm	Attributes	Applicable major release
Name: SLCBOOTCONTCOM (4925) Type: configurationAlarm Package: equipment.SLCBOOTCONTCOM Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCBOOTCONTCOM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC Booting Communication failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-582 SLCCARDINIT

Alarm	Attributes	Applicable major release
Name: SLCCARDINIT (4926) Type: configurationAlarm Package: equipment.SLCCARDINIT Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCCARDINIT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC initializing .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-583 SLCCLKSYNC

Alarm	Attributes	Applicable major release
Name: SLCCLKSYNC (4927) Type: configurationAlarm Package: equipment.SLCCLKSYNC Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCCLKSYNC	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC Clock Sync in progress .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-584 SLCCONTCOM

Alarm	Attributes	Applicable major release
Name: SLCCONTCOM (4928) Type: configurationAlarm Package: equipment.SLCCONTCOM Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCCONTCOM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC failure - communication .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-585 SLCDATAFLT

Alarm	Attributes	Applicable major release
Name: SLCDATAFLT (4929) Type: configurationAlarm Package: equipment.SLCDATAFLT Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCDATAFLT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC provisioning failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-586 SLCEQPTBOOT

Alarm	Attributes	Applicable major release
Name: SLCEQPTBOOT (4930) Type: configurationAlarm Package: equipment.SLCEQPTBOOT Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCEQPTBOOT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC Card failure - infra/boot failure .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-587 SLCMISMATCH

Alarm	Attributes	Applicable major release
Name: SLCMISMATCH (4931) Type: configurationAlarm Package: equipment.SLCMISMATCH Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCMISMATCH	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC Software version mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-588 SLCNOTINSERVICE

Alarm	Attributes	Applicable major release
Name: SLCNOTINSERVICE (4932) Type: configurationAlarm Package: equipment.SLCNOTINSERVICE Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLCNOTINSERVICE	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SLC Card not in service .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-589 SLTMSIG

Alarm	Attributes	Applicable major release
Name: SLTMSIG (3735) Type: equipmentAlarm Package: optical.SLTMSIG Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SLTMSIG	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Timing reference out-of-frequency is detected.		
Remedial action: To clear the alarm, check the reference frequency offset.		

Table 3-590 SNCInAutomaticRestorationDisabledMode

Alarm	Attributes	Applicable major release
Name: SNCInAutomaticRestorationDisabledMode (8245) Type: communicationsAlarm Package: gmpls.SNCInAutomaticRestorationDisabledMode Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SNCInAutomaticRestorationDisabledMode	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when automatic restoration is disabled for this LSP.		
Remedial action: Not Available.		

Table 3-591 SNCPDegraded

Alarm	Attributes	Applicable major release
Name: SNCPDegraded (8246) Type: communicationsAlarm Package: gmpls.SNCPDegraded Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SNCPDegraded	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the LSP is not 1+1 path protected.		
Remedial action: Not Available.		

Table 3-592 SoftwareError

Alarm	Attributes	Applicable major release
Name: SoftwareError (11129) Type: softwareAlarm Package: equipment.SoftwareError Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SoftwareError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Software Error reported .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-593 SoftwareNotCommitted

Alarm	Attributes	Applicable major release
Name: SoftwareNotCommitted (4871) Type: communicationsAlarm Package: netw.SoftwareNotCommitted Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwUpgCommit	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when No committed software load Autoinstall disabled is detected.		
Remedial action: For 1830 PSS Node, To upgrade to a new release or clear the alarm, the current software load must be committed. Enter the following command to commit the software: CLI config software upgrade commit.		

Table 3-594 SoftwareUpgradeFailure

Alarm	Attributes	Applicable major release
Name: SoftwareUpgradeFailure (2899) Type: equipmentAlarm Package: netw.SoftwareUpgradeFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwUpgFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Software upgrade failed is detected.		
Remedial action: For 1830 PSS Node.Refer section SWUPGFAIL (Software Upgrade Failed) in 1830 TroubleShooting guide.		

Table 3-595 SoftwareUpgradeInProgress

Alarm	Attributes	Applicable major release
Name: SoftwareUpgradeInProgress (2900) Type: equipmentAlarm Package: netw.SoftwareUpgradeInProgress Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwftDwn	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Software upgrade in progress is detected.		
Remedial action: Informational.		

Table 3-596 SoftwareVersionMismatch

Alarm	Attributes	Applicable major release
Name: SoftwareVersionMismatch (2092) Type: communicationsAlarm Package: equipment.SoftwareVersionMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfMismatch Applicable probable causes: • SfMismatch • SWMISM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Software version mismatch is detected.		

Table 3-596 SoftwareVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised under the following conditions:\n a. The software on the alarmed card does not match the software on the nearest EC card because the card failed to update successfully.\n b. When all cards are not running the same software release. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Find the software version number and release number on the EC card. Compare the corresponding number in the alarmed card. If it is not the same, download the software from EC to the alarmed card.\n 2. Contact your Nokia support representative.		

Table 3-597 SonetAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetAlarmIndicationSignal (4555) Type: communicationsAlarm Package: equipment.SonetAlarmIndicationSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AisL Applicable probable causes: • AisL • AisLM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when AIS Line/MS is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-598 SonetLineRemoteFailureIndication

Alarm	Attributes	Applicable major release
Name: SonetLineRemoteFailureIndication (4556) Type: communicationsAlarm Package: equipment. SonetLineRemoteFailureIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RfiL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when RFI Line/MS is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-599 SonetLossOfClock

Alarm	Attributes	Applicable major release
Name: SonetLossOfClock (4557) Type: communicationsAlarm Package: equipment.SonetLossOfClock Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LostClock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-600 SonetLossOfFrame

Alarm	Attributes	Applicable major release
Name: SonetLossOfFrame (2093) Type: communicationsAlarm Package: equipment.SonetLossOfFrame Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Lof	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of frame is detected.		
Remedial action: A receive port on one of the optical cards has detected a Loss Of Frame. The LOF alarm is raised if:the SONET framer detects framing errors in the A1/A2 overhead bytes as per the SONET specification the OTN framer detects corruption in the Framing Alignment Signal (FAS) bytes.Please refer LOF (Loss Of Frame) section for detailed corrective action in 1830 Troubleshooting guide.		

Table 3-601 SonetLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetLossOfPointer (4558) Type: communicationsAlarm Package: equipment.SonetLossOfPointer Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LostClock	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of clock is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-602 SonetLossOfSignal

Alarm	Attributes	Applicable major release
Name: SonetLossOfSignal (4559) Type: communicationsAlarm Package: equipment.SonetLossOfSignal Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Los	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of signal is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-603 SonetSectionTraceMismatch

Alarm	Attributes	Applicable major release
Name: SonetSectionTraceMismatch (2094) Type: communicationsAlarm Package: equipment.SonetSectionTraceMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Tim	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trace Identifier Mismatch is detected.		
Remedial action: This alarm indicates that the received trail trace is not the same as the expected trail trace.\n For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-604 SonetSignalDegrade

Alarm	Attributes	Applicable major release
Name: SonetSignalDegrade (4560) Type: communicationsAlarm Package: equipment.SonetSignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sd	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Signal Degrade is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-605 SonetSignalFailure

Alarm	Attributes	Applicable major release
Name: SonetSignalFailure (4561) Type: communicationsAlarm Package: equipment.SonetSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Sf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Excessive BER is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-606 SpiReadError

Alarm	Attributes	Applicable major release
Name: SpiReadError (8168) Type: equipmentAlarm Package: equipment.SpiReadError Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SpiReadError	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Equipage SPI bus read errors.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-607 SpLoAdjFail

Alarm	Attributes	Applicable major release
Name: SpLoAdjFail (3393) Type: communicationsAlarm Package: equipment.SpLoAdjFail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SpLoAdjFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Span Loss Adjustment Failure is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-608 SrgDiviersity

Alarm	Attributes	Applicable major release
Name: SrgDiviersity (5589) Type: communicationsAlarm Package: netw.SrgDiviersity Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SrgDiviersity	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SRG diversity violation.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-609 SRGViolation

Alarm	Attributes	Applicable major release
Name: SRGViolation (8247) Type: communicationsAlarm Package: gmpls.SRGViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SRGViolation	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when both legs (SNCP) of the LSP or the LSP to its diverse LSP are not SRG diverse. Also after a cut scenario if a new backup could not be SRG diverse (only link diverse) to the failure, the violation is raised.		
Remedial action: Not Available.		

Table 3-610 SsfCltEgr

Alarm	Attributes	Applicable major release
Name: SsfCltEgr (3969) Type: communicationsAlarm Package: equipment.SsfCltEgr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SsfCltEgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Egress Server Signal Failure - Client is detected.		
Remedial action: Proceed to Procedure - Clear Egress Server Signal Failure-Client in 1830 Troubleshooting guide.		

Table 3-611 SsfOduOut

Alarm	Attributes	Applicable major release
Name: SsfOduOut (4562) Type: communicationsAlarm Package: equipment.SsfOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SsfOduOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Server Signal Failure - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-612 SsfSection

Alarm	Attributes	Applicable major release
Name: SsfSection (4563) Type: communicationsAlarm Package: equipment.SsfSection Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SsfSection	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure - Section is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-613 SsfSectionOut

Alarm	Attributes	Applicable major release
Name: SsfSectionOut (4935) Type: communicationsAlarm Package: equipment.SsfSectionOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SsfSectionOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Server Signal Failure - Section .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-614 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 3-615 SubNodeUnreachable

Alarm	Attributes	Applicable major release
Name: SubNodeUnreachable (5590) Type: communicationsAlarm Package: netw.SubNodeUnreachable Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SubNodeUnreachable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Logical node not reachable.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-616 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 3-617 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-617 SubSysChassMemoryUsageHi (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 3-618 SubtendedShelfIdAssignmentFailure

Alarm	Attributes	Applicable major release
Name: SubtendedShelfIdAssignmentFailure (4872) Type: equipmentAlarm Package: netw.SubtendedShelfIdAssignmentFailure Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrcdrErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a subtended shelf cannot be assigned a shelf ID.		
Remedial action: Please refer section PRCDRERR in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-619 SupvySignalDegrade

Alarm	Attributes	Applicable major release
Name: SupvySignalDegrade (4564) Type: communicationsAlarm Package: equipment.SupvySignalDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdegO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SUPVY Signal Degrade is detected.		
Remedial action: This alarm is raised when OSC SFP receive port on one of the amplifier cards has detected a signal degrade.\n For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-620 SuspectClkFreq

Alarm	Attributes	Applicable major release
Name: SuspectClkFreq (5449) Type: communicationsAlarm Package: equipment.SuspectClkFreq Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SuspectClkFreq	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Freq error > 9.2 ppm ="=> downstream wavetracker errors ."		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-621 SyncChannelA

Alarm	Attributes	Applicable major release
Name: SyncChannelA (11130) Type: equipmentAlarm Package: equipment.SyncChannelA Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntSyncA	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal Synchronization Signal fail from CRU A .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-622 SyncChannelB

Alarm	Attributes	Applicable major release
Name: SyncChannelB (11131) Type: equipmentAlarm Package: equipment.SyncChannelB Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntSyncB	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal Synchronization Signal fail from CRU B .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-623 SyncChannelBoth

Alarm	Attributes	Applicable major release
Name: SyncChannelBoth (11132) Type: equipmentAlarm Package: equipment.SyncChannelBoth Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntSyncBoth	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Internal Synchronization Signal fail from both CRU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-624 SyncEqpt

Alarm	Attributes	Applicable major release
Name: SyncEqpt (4565) Type: equipmentAlarm Package: equipment.SyncEqpt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncEqpt	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Synchronization equipment failure is detected.		
Remedial action: Refer Procedure : Clear Synchronization Equipment (CRU) failure alarm in 1830 Troubleshooting guide.		

Table 3-625 SyncIfTimingHoldover

Alarm	Attributes	Applicable major release
Name: SyncIfTimingHoldover (3970) Type: equipmentAlarm Package: equipment.SyncIfTimingHoldover Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncIfTimingHoldover	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Sync Timing Holdover is detected.		
Remedial action: Please refer section - System Timing is in Autonomous Holdover Synchronization Mode in 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-626 SyncIfTimingRef1Alarm

Alarm	Attributes	Applicable major release
Name: SyncIfTimingRef1Alarm (3971) Type: equipmentAlarm Package: equipment.SyncIfTimingRef1Alarm Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncIfTimingRef1Alarm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Sync Timing LineRef0 Alarm is detected.		
Remedial action: This means Synchronization timing reference one has an alarm condition.Please refer section - Sync Timing Reference Failure in 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-627 SyncIfTimingRef2Alarm

Alarm	Attributes	Applicable major release
Name: SyncIfTimingRef2Alarm (3972) Type: equipmentAlarm Package: equipment.SyncIfTimingRef2Alarm Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncIfTimingRef2Alarm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Sync Timing LineRef1 Alarm is detected.		
Remedial action: This means Synchronization timing reference two has an alarm condition.Please refer section - Sync Timing Reference Failure in 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-628 SyncLoss

Alarm	Attributes	Applicable major release
Name: SyncLoss (4956) Type: communicationsAlarm Package: ptp.SyncLoss Raised on class: ptp.IEEEPTPPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncLoss	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Sync messages on the slave port .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-629 SyncMisc1

Alarm	Attributes	Applicable major release
Name: SyncMisc1 (8445) Type: equipmentAlarm Package: equipment.SyncMisc1 Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncMisc1	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The standby CRU fails to synchronize		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-630 SyncOos

Alarm	Attributes	Applicable major release
Name: SyncOos (3919) Type: equipmentAlarm Package: equipment.SyncOos Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncOos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when All selectable timing reference fail is detected.		
Remedial action: SYNCOOS (Timing reference failed (Not Protected or Protection not Available)) / SYNCOOS (Timing reference failed--system going into holdover).Check the timing reference quality and priority.Also, Check the reference status.		

Table 3-631 SyncOosT4

Alarm	Attributes	Applicable major release
Name: SyncOosT4 (4566) Type: equipmentAlarm Package: equipment.SyncOosT4 Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncOos_T4	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when T4:All selectable timing reference fail is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-632 SyncRefFail

Alarm	Attributes	Applicable major release
Name: SyncRefFail (3736) Type: equipmentAlarm Package: optical.SyncRefFail Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncRefFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when timing reference fails. .		
Remedial action: Check the timing reference quality and priority.		

Table 3-633 SyncRefUnEq

Alarm	Attributes	Applicable major release
Name: SyncRefUnEq (3926) Type: equipmentAlarm Package: optical.SyncRefUnEq Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncRefUnEq	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Timing reference is unassigned is detected.		
Remedial action: Check the reference assignment.		

Table 3-634 SyncT4Out

Alarm	Attributes	Applicable major release
Name: SyncT4Out (4567) Type: equipmentAlarm Package: equipment.SyncT4Out Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncT4Out	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Timing quality for output timing is insufficient and therefore squelched is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-635 SystemTimingCardMismatch

Alarm	Attributes	Applicable major release
Name: SystemTimingCardMismatch (4568) Type: equipmentAlarm Package: equipment.SystemTimingCardMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing card mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-636 SystemTimingLossOfBothClocks

Alarm	Attributes	Applicable major release
Name: SystemTimingLossOfBothClocks (4569) Type: equipmentAlarm Package: equipment.SystemTimingLossOfBothClocks Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncSysOos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing loss of both clocks is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-637 SystemTimingLossOfClockRedundancy

Alarm	Attributes	Applicable major release
Name: SystemTimingLossOfClockRedundancy (4570) Type: equipmentAlarm Package: equipment.SystemTimingLossOfClockRedundancy Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncSys	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing loss of clock redundancy - Clock A missing is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-638 SystemTimingMisconfiguration

Alarm	Attributes	Applicable major release
Name: SystemTimingMisconfiguration (4873) Type: communicationsAlarm Package: netw.SystemTimingMisconfiguration Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrcdrErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when System timing misprovisioning is detected.		
Remedial action: Please refer section PRCDRERR in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-639 TBbeMs15Min

Alarm	Attributes	Applicable major release
Name: TBbeMs15Min (3396) Type: qualityOfServiceAlarm Package: equipment.TBbeMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-640 TBbeMs1Day

Alarm	Attributes	Applicable major release
Name: TBbeMs1Day (3397) Type: qualityOfServiceAlarm Package: equipment.TBbeMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-641 TBbeOdu15Min

Alarm	Attributes	Applicable major release
Name: TBbeOdu15Min (3398) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-642 TBbeOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TBbeOdu15MinOut (8446) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-643 TBbeOdu1Day

Alarm	Attributes	Applicable major release
Name: TBbeOdu1Day (3399) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-644 TBbeOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TBbeOdu1DayOut (8447) Type: qualityOfServiceAlarm Package: equipment.TBbeOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-645 TBbeOtu15Min

Alarm	Attributes	Applicable major release
Name: TBbeOtu15Min (3400) Type: qualityOfServiceAlarm Package: equipment.TBbeOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-646 TBbeOtu1Day

Alarm	Attributes	Applicable major release
Name: TBbeOtu1Day (3401) Type: qualityOfServiceAlarm Package: equipment.TBbeOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-647 TBbeP15Min

Alarm	Attributes	Applicable major release
Name: TBbeP15Min (3402) Type: qualityOfServiceAlarm Package: equipment.TBbeP15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_P_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-648 TBbeP1Day

Alarm	Attributes	Applicable major release
Name: TBbeP1Day (3403) Type: qualityOfServiceAlarm Package: equipment.TBbeP1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_P_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-649 TBbePt15Min

Alarm	Attributes	Applicable major release
Name: TBbePt15Min (3404) Type: qualityOfServiceAlarm Package: equipment.TBbePt15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_PT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-650 TBbePt1Day

Alarm	Attributes	Applicable major release
Name: TBbePt1Day (3405) Type: qualityOfServiceAlarm Package: equipment.TBbePt1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_PT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-651 TBbeRs15Min

Alarm	Attributes	Applicable major release
Name: TBbeRs15Min (3406) Type: qualityOfServiceAlarm Package: equipment.TBbeRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-652 TBbeRs1Day

Alarm	Attributes	Applicable major release
Name: TBbeRs1Day (3407) Type: qualityOfServiceAlarm Package: equipment.TBbeRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-653 TBbeRst15Min

Alarm	Attributes	Applicable major release
Name: TBbeRst15Min (3408) Type: qualityOfServiceAlarm Package: equipment.TBbeRst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-654 TBbeRst1Day

Alarm	Attributes	Applicable major release
Name: TBbeRst1Day (3409) Type: qualityOfServiceAlarm Package: equipment.TBbeRst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_RST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-655 TBbeTcm15Min

Alarm	Attributes	Applicable major release
Name: TBbeTcm15Min (4573) Type: qualityOfServiceAlarm Package: equipment.TBbeTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-656 TBbeTcm1Day

Alarm	Attributes	Applicable major release
Name: TBbeTcm1Day (4574) Type: qualityOfServiceAlarm Package: equipment.TBbeTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BBE_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-657 TBerPostFec15Min

Alarm	Attributes	Applicable major release
Name: TBerPostFec15Min (3410) Type: qualityOfServiceAlarm Package: equipment.TBerPostFec15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BERPOSTFEC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a postFEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-658 TBerPostFec1Day

Alarm	Attributes	Applicable major release
Name: TBerPostFec1Day (3411) Type: qualityOfServiceAlarm Package: equipment.TBerPostFec1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BERPOSTFEC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a postFEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-659 TBerPreFec15Min

Alarm	Attributes	Applicable major release
Name: TBerPreFec15Min (3412) Type: qualityOfServiceAlarm Package: equipment.TBerPreFec15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BERPREFEC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a preFEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-660 TBerPreFec1Day

Alarm	Attributes	Applicable major release
Name: TBerPreFec1Day (3413) Type: qualityOfServiceAlarm Package: equipment.TBerPreFec1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BERPREFEC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a preFEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-661 TBIAESOtu15Min

Alarm	Attributes	Applicable major release
Name: TBIAESOtu15Min (3394) Type: qualityOfServiceAlarm Package: equipment.TBIAESOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BIAES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BIAES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-662 TBIAESOtu1Day

Alarm	Attributes	Applicable major release
Name: TBIAESOtu1Day (3395) Type: qualityOfServiceAlarm Package: equipment.TBIAESOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BIAES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BIAES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-663 TBIAESTcm15Min

Alarm	Attributes	Applicable major release
Name: TBIAESTcm15Min (4571) Type: qualityOfServiceAlarm Package: equipment.TBIAESTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BIAES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BIAES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-664 TBIAESTcm1Day

Alarm	Attributes	Applicable major release
Name: TBIAESTcm1Day (4572) Type: qualityOfServiceAlarm Package: equipment.TBIAESTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_BIAES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BIAES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-665 TCAChannelMargin

Alarm	Attributes	Applicable major release
Name: TCAChannelMargin (9630) Type: qualityOfServiceAlarm Package: gmpls.TCAChannelMargin Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TCAChannelMargin	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the Qos threshold of the path has been exceeded.		
Remedial action: Not Available.		

Table 3-666 TCMAis

Alarm	Attributes	Applicable major release
Name: TCMAis (5450) Type: communicationsAlarm Package: equipment.TCMAis Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TCMAis	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when TCM-AIS .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-667 TcmBackwardDefectIndication

Alarm	Attributes	Applicable major release
Name: TcmBackwardDefectIndication (4591) Type: communicationsAlarm Package: equipment.TcmBackwardDefectIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BdiTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Backward Defect Indication - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-668 TcmLockedIndication

Alarm	Attributes	Applicable major release
Name: TcmLockedIndication (4592) Type: communicationsAlarm Package: equipment.TcmLockedIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LckTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Locked - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-669 TcmLossofTandemConnection

Alarm	Attributes	Applicable major release
Name: TcmLossofTandemConnection (4593) Type: communicationsAlarm Package: equipment.TcmLossofTandemConnection Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LtcTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Tandem Connection - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-670 TcmOpenConnectionIndication

Alarm	Attributes	Applicable major release
Name: TcmOpenConnectionIndication (4594) Type: communicationsAlarm Package: equipment.TcmOpenConnectionIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OciTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Open Connection Indication - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-671 TcmServerSignalFailure

Alarm	Attributes	Applicable major release
Name: TcmServerSignalFailure (4595) Type: communicationsAlarm Package: equipment.TcmServerSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SsfTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Server Signal Failure - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-672 TcmTrailTraceIdentifierMismatch

Alarm	Attributes	Applicable major release
Name: TcmTrailTraceIdentifierMismatch (4596) Type: communicationsAlarm Package: equipment.TcmTrailTraceIdentifierMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TimTcm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trail Identifier Mismatch - TCM is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-673 TCv15Min

Alarm	Attributes	Applicable major release
Name: TCv15Min (3414) Type: qualityOfServiceAlarm Package: equipment.TCv15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-674 TCv1Day

Alarm	Attributes	Applicable major release
Name: TCv1Day (3415) Type: qualityOfServiceAlarm Package: equipment.TCv1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-675 TCvPcs15Min

Alarm	Attributes	Applicable major release
Name: TCvPcs15Min (3416) Type: qualityOfServiceAlarm Package: equipment.TCvPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-676 TCvPcs1Day

Alarm	Attributes	Applicable major release
Name: TCvPcs1Day (3417) Type: qualityOfServiceAlarm Package: equipment.TCvPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-677 TCvPcst15Min

Alarm	Attributes	Applicable major release
Name: TCvPcst15Min (3418) Type: qualityOfServiceAlarm Package: equipment.TCvPcst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-678 TCvPcst1Day

Alarm	Attributes	Applicable major release
Name: TCvPcst1Day (3419) Type: qualityOfServiceAlarm Package: equipment.TCvPcst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-679 TCvs15Min

Alarm	Attributes	Applicable major release
Name: TCvs15Min (3420) Type: qualityOfServiceAlarm Package: equipment.TCvs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CVS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-680 TCvs1Day

Alarm	Attributes	Applicable major release
Name: TCvs1Day (3421) Type: qualityOfServiceAlarm Package: equipment.TCvs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CVS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-681 TCvst15Min

Alarm	Attributes	Applicable major release
Name: TCvst15Min (3422) Type: qualityOfServiceAlarm Package: equipment.TCvst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CVST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-682 TCvst1Day

Alarm	Attributes	Applicable major release
Name: TCvst1Day (3423) Type: qualityOfServiceAlarm Package: equipment.TCvst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CVST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a CV-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-683 TerminalLoopbackConfigured (equipment)

Alarm	Attributes	Applicable major release
Name: TerminalLoopbackConfigured (8381) Type: communicationsAlarm Package: equipment.TerminalLoopbackConfigured Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TerminalLoopbackConfigured	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Terminal Loopback is configured on Port.		
Remedial action: To clear the condition, disable Terminal Loopback configured on port.		

Table 3-684 TEs15Min

Alarm	Attributes	Applicable major release
Name: TEs15Min (3424) Type: qualityOfServiceAlarm Package: equipment.TEs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-685 TEs1Day

Alarm	Attributes	Applicable major release
Name: TEs1Day (3425) Type: qualityOfServiceAlarm Package: equipment.TEs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-686 TEsL15Min

Alarm	Attributes	Applicable major release
Name: TEsL15Min (3426) Type: qualityOfServiceAlarm Package: equipment.TEsL15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_L_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-L Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-687 TEsL1Day

Alarm	Attributes	Applicable major release
Name: TEsL1Day (3427) Type: qualityOfServiceAlarm Package: equipment.TEsL1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_L_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-L Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-688 TEsMs15Min

Alarm	Attributes	Applicable major release
Name: TEsMs15Min (3428) Type: qualityOfServiceAlarm Package: equipment.TEsMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-689 TEsMs1Day

Alarm	Attributes	Applicable major release
Name: TEsMs1Day (3429) Type: qualityOfServiceAlarm Package: equipment.TEsMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-690 TEsOdu15Min

Alarm	Attributes	Applicable major release
Name: TEsOdu15Min (3430) Type: qualityOfServiceAlarm Package: equipment.TEsOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-691 TEsOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TEsOdu15MinOut (8448) Type: qualityOfServiceAlarm Package: equipment.TEsOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-692 TEsOdu1Day

Alarm	Attributes	Applicable major release
Name: TEsOdu1Day (3431) Type: qualityOfServiceAlarm Package: equipment.TEsOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-693 TEsOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TEsOdu1DayOut (8449) Type: qualityOfServiceAlarm Package: equipment.TEsOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-694 TEsOtu15Min

Alarm	Attributes	Applicable major release
Name: TEsOtu15Min (3432) Type: qualityOfServiceAlarm Package: equipment.TEsOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-695 TEsOtu1Day

Alarm	Attributes	Applicable major release
Name: TEsOtu1Day (3433) Type: qualityOfServiceAlarm Package: equipment.TEsOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-696 TEsP15Min

Alarm	Attributes	Applicable major release
Name: TEsP15Min (3434) Type: qualityOfServiceAlarm Package: equipment.TEsP15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_P_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-697 TEsP1Day

Alarm	Attributes	Applicable major release
Name: TEsP1Day (3435) Type: qualityOfServiceAlarm Package: equipment.TEsP1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_P_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-698 TEsPcs15Min

Alarm	Attributes	Applicable major release
Name: TEsPcs15Min (3436) Type: qualityOfServiceAlarm Package: equipment.TEsPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-699 TEsPcs1Day

Alarm	Attributes	Applicable major release
Name: TEsPcs1Day (3437) Type: qualityOfServiceAlarm Package: equipment.TEsPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-700 TEsPcst15Min

Alarm	Attributes	Applicable major release
Name: TEsPcst15Min (3438) Type: qualityOfServiceAlarm Package: equipment.TEsPcst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-701 TEsPcst1Day

Alarm	Attributes	Applicable major release
Name: TEsPcst1Day (3439) Type: qualityOfServiceAlarm Package: equipment.TEsPcst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-702 TEsPt15Min

Alarm	Attributes	Applicable major release
Name: TEsPt15Min (3440) Type: qualityOfServiceAlarm Package: equipment.TEsPt15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-703 TEsPt1Day

Alarm	Attributes	Applicable major release
Name: TEsPt1Day (3441) Type: qualityOfServiceAlarm Package: equipment.TEsPt1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-704 TEsRs15Min

Alarm	Attributes	Applicable major release
Name: TEsRs15Min (3442) Type: qualityOfServiceAlarm Package: equipment.TEsRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-705 TEsRs1Day

Alarm	Attributes	Applicable major release
Name: TEsRs1Day (3443) Type: qualityOfServiceAlarm Package: equipment.TEsRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-706 TEsRst15Min

Alarm	Attributes	Applicable major release
Name: TEsRst15Min (3444) Type: qualityOfServiceAlarm Package: equipment.TEsRst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-707 TEsRst1Day

Alarm	Attributes	Applicable major release
Name: TEsRst1Day (3445) Type: qualityOfServiceAlarm Package: equipment.TEsRst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_RST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-708 TEss15Min

Alarm	Attributes	Applicable major release
Name: TEss15Min (3446) Type: qualityOfServiceAlarm Package: equipment.TEss15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ESS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-709 TEss1Day

Alarm	Attributes	Applicable major release
Name: TEss1Day (3447) Type: qualityOfServiceAlarm Package: equipment.TEss1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ESS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-710 TEsst15Min

Alarm	Attributes	Applicable major release
Name: TEsst15Min (3448) Type: qualityOfServiceAlarm Package: equipment.TEsst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ESST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-711 TEsst1Day

Alarm	Attributes	Applicable major release
Name: TEsst1Day (3449) Type: qualityOfServiceAlarm Package: equipment.TEsst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ESST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-712 TEsTcm15Min

Alarm	Attributes	Applicable major release
Name: TEsTcm15Min (4575) Type: qualityOfServiceAlarm Package: equipment.TEsTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-713 TEsTcm1Day

Alarm	Attributes	Applicable major release
Name: TEsTcm1Day (4576) Type: qualityOfServiceAlarm Package: equipment.TEsTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-714 TestMode

Alarm	Attributes	Applicable major release
Name: TestMode (5591) Type: communicationsAlarm Package: netw.TestMode Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TestMode	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when test mode.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-715 TestModeEnabled

Alarm	Attributes	Applicable major release
Name: TestModeEnabled (8249) Type: communicationsAlarm Package: gmpls.TestModeEnabled Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TestModeEnabled	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the LSP is in test mode and 'frozen' to its current route.		
Remedial action: Not Available.		

Table 3-716 TEthpkter15Min

Alarm	Attributes	Applicable major release
Name: TEthpkter15Min (3450) Type: qualityOfServiceAlarm Package: equipment.TEthpkter15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ETHPKTER_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ETHPKTER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-717 TEthpkter1Day

Alarm	Attributes	Applicable major release
Name: TEthpkter1Day (3451) Type: qualityOfServiceAlarm Package: equipment.TEthpkter1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ETHPKTER_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ETHPKTER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-718 TEthpktert15Min

Alarm	Attributes	Applicable major release
Name: TEthpktert15Min (3452) Type: qualityOfServiceAlarm Package: equipment.TEthpktert15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ETHPKTERT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ETHPKTERT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-719 TEthpktert1Day

Alarm	Attributes	Applicable major release
Name: TEthpktert1Day (3453) Type: qualityOfServiceAlarm Package: equipment.TEthpktert1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ETHPKTERT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ETHPKTERT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-720 TFeBbeMs15Min

Alarm	Attributes	Applicable major release
Name: TFeBbeMs15Min (3454) Type: qualityOfServiceAlarm Package: equipment.TFeBbeMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEBBE-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-721 TFeBbeMs1Day

Alarm	Attributes	Applicable major release
Name: TFeBbeMs1Day (3455) Type: qualityOfServiceAlarm Package: equipment.TFeBbeMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEBBE-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-722 TFeBbeOdu15Min

Alarm	Attributes	Applicable major release
Name: TFeBbeOdu15Min (3456) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-723 TFeBbeOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TFeBbeOdu15MinOut (8450) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-724 TFeBbeOdu1Day

Alarm	Attributes	Applicable major release
Name: TFeBbeOdu1Day (3457) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-725 TFeBbeOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TFeBbeOdu1DayOut (8451) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-726 TFeBbeOtu15Min

Alarm	Attributes	Applicable major release
Name: TFeBbeOtu15Min (3458) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-727 TFeBbeOtu1Day

Alarm	Attributes	Applicable major release
Name: TFeBbeOtu1Day (3459) Type: qualityOfServiceAlarm Package: equipment.TFeBbeOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd BBE-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-728 TFeBbeTcm15Min

Alarm	Attributes	Applicable major release
Name: TFeBbeTcm15Min (4577) Type: qualityOfServiceAlarm Package: equipment.TFeBbeTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-729 TFeBbeTcm1Day

Alarm	Attributes	Applicable major release
Name: TFeBbeTcm1Day (4578) Type: qualityOfServiceAlarm Package: equipment.TFeBbeTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEBBE_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a BBE-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-730 TFecc15Min

Alarm	Attributes	Applicable major release
Name: TFecc15Min (3480) Type: qualityOfServiceAlarm Package: equipment.TFecc15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FECC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-731 TFecc1Day

Alarm	Attributes	Applicable major release
Name: TFecc1Day (3481) Type: qualityOfServiceAlarm Package: equipment.TFecc1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FECC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-732 TFecUbc15Min

Alarm	Attributes	Applicable major release
Name: TFecUbc15Min (4936) Type: communicationsAlarm Package: equipment.TFecUbc15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEC_UBC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECUBC Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-733 TFecUbc1Day

Alarm	Attributes	Applicable major release
Name: TFecUbc1Day (4937) Type: communicationsAlarm Package: equipment.TFecUbc1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEC_UBC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECUBC Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-734 TFecUbu15Min

Alarm	Attributes	Applicable major release
Name: TFecUbu15Min (3478) Type: qualityOfServiceAlarm Package: equipment.TFecUbu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEC_UBU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECUBC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-735 TFecUbu1Day

Alarm	Attributes	Applicable major release
Name: TFecUbu1Day (3479) Type: qualityOfServiceAlarm Package: equipment.TFecUbu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEC_UBU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FECUBC Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-736 TFeEsMs15Min

Alarm	Attributes	Applicable major release
Name: TFeEsMs15Min (3460) Type: qualityOfServiceAlarm Package: equipment.TFeEsMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-737 TFeEsMs1Day

Alarm	Attributes	Applicable major release
Name: TFeEsMs1Day (3461) Type: qualityOfServiceAlarm Package: equipment.TFeEsMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-738 TFeEsOdu15Min

Alarm	Attributes	Applicable major release
Name: TFeEsOdu15Min (3462) Type: qualityOfServiceAlarm Package: equipment.TFeEsOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-739 TFeEsOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TFeEsOdu15MinOut (8452) Type: qualityOfServiceAlarm Package: equipment.TFeEsOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-740 TFeEsOdu1Day

Alarm	Attributes	Applicable major release
Name: TFeEsOdu1Day (3463) Type: qualityOfServiceAlarm Package: equipment.TFeEsOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-741 TFeEsOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TFeEsOdu1DayOut (8453) Type: qualityOfServiceAlarm Package: equipment.TFeEsOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-742 TFeEsOtu15Min

Alarm	Attributes	Applicable major release
Name: TFeEsOtu15Min (3464) Type: qualityOfServiceAlarm Package: equipment.TFeEsOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-743 TFeEsOtu1Day

Alarm	Attributes	Applicable major release
Name: TFeEsOtu1Day (3465) Type: qualityOfServiceAlarm Package: equipment.TFeEsOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd ES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-744 TFeEsTcm15Min

Alarm	Attributes	Applicable major release
Name: TFeEsTcm15Min (4579) Type: qualityOfServiceAlarm Package: equipment.TFeEsTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-745 TFeEsTcm1Day

Alarm	Attributes	Applicable major release
Name: TFeEsTcm1Day (4580) Type: qualityOfServiceAlarm Package: equipment.TFeEsTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a ES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-746 TFeSesMs15Min

Alarm	Attributes	Applicable major release
Name: TFeSesMs15Min (3466) Type: qualityOfServiceAlarm Package: equipment.TFeSesMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FESES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-747 TFeSesMs1Day

Alarm	Attributes	Applicable major release
Name: TFeSesMs1Day (3467) Type: qualityOfServiceAlarm Package: equipment.TFeSesMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FESES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-748 TFeSesOdu15Min

Alarm	Attributes	Applicable major release
Name: TFeSesOdu15Min (3468) Type: qualityOfServiceAlarm Package: equipment.TFeSesOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-749 TFeSesOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TFeSesOdu15MinOut (8454) Type: qualityOfServiceAlarm Package: equipment.TFeSesOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-750 TFeSesOdu1Day

Alarm	Attributes	Applicable major release
Name: TFeSesOdu1Day (3469) Type: qualityOfServiceAlarm Package: equipment.TFeSesOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-751 TFeSesOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TFeSesOdu1DayOut (8455) Type: qualityOfServiceAlarm Package: equipment.TFeSesOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-752 TFeSesOtu15Min

Alarm	Attributes	Applicable major release
Name: TFeSesOtu15Min (3470) Type: qualityOfServiceAlarm Package: equipment.TFeSesOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-753 TFeSesOtu1Day

Alarm	Attributes	Applicable major release
Name: TFeSesOtu1Day (3471) Type: qualityOfServiceAlarm Package: equipment.TFeSesOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-754 TFeSesTcm15Min

Alarm	Attributes	Applicable major release
Name: TFeSesTcm15Min (4581) Type: qualityOfServiceAlarm Package: equipment.TFeSesTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-755 TFeSesTcm1Day

Alarm	Attributes	Applicable major release
Name: TFeSesTcm1Day (4582) Type: qualityOfServiceAlarm Package: equipment.TFeSesTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FESES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-756 TFeUasMs15Min

Alarm	Attributes	Applicable major release
Name: TFeUasMs15Min (3472) Type: qualityOfServiceAlarm Package: equipment.TFeUasMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEUAS-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-757 TFeUasMs1Day

Alarm	Attributes	Applicable major release
Name: TFeUasMs1Day (3473) Type: qualityOfServiceAlarm Package: equipment.TFeUasMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FEUAS-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-758 TFeUasOdu15Min

Alarm	Attributes	Applicable major release
Name: TFeUasOdu15Min (3474) Type: qualityOfServiceAlarm Package: equipment.TFeUasOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-759 TFeUasOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TFeUasOdu15MinOut (8456) Type: qualityOfServiceAlarm Package: equipment.TFeUasOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-760 TFeUasOdu1Day

Alarm	Attributes	Applicable major release
Name: TFeUasOdu1Day (3475) Type: qualityOfServiceAlarm Package: equipment.TFeUasOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-761 TFeUasOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TFeUasOdu1DayOut (8457) Type: qualityOfServiceAlarm Package: equipment.TFeUasOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-762 TFeUasOtu15Min

Alarm	Attributes	Applicable major release
Name: TFeUasOtu15Min (3476) Type: qualityOfServiceAlarm Package: equipment.TFeUasOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-763 TFeUasOtu1Day

Alarm	Attributes	Applicable major release
Name: TFeUasOtu1Day (3477) Type: qualityOfServiceAlarm Package: equipment.TFeUasOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a FarEnd UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-764 TFeUasTcm15Min

Alarm	Attributes	Applicable major release
Name: TFeUasTcm15Min (4583) Type: qualityOfServiceAlarm Package: equipment.TFeUasTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates an UAS-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-765 TFeUasTcm1Day

Alarm	Attributes	Applicable major release
Name: TFeUasTcm1Day (4584) Type: qualityOfServiceAlarm Package: equipment.TFeUasTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_FEUAS_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates an UAS-ODU-TCM FarEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-766 ThresholdCrossingAlarmCfmTwoWayDelayTest

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmCfmTwoWayDelayTest (4943) Type: thresholdCrossed Package: ethernetoam. ThresholdCrossingAlarmCfmTwoWayDelayTest Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Test attribute crosses a TCA threshold on this object.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 3-767 ThresholdCrossingAlarmCfmTwoWaySlm

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmCfmTwoWaySlm (4944) Type: thresholdCrossed Package: ethernetoam. ThresholdCrossingAlarmCfmTwoWaySlm Raised on class: ethernetoam.CfmTwoWaySlm	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a test attribute crosses a TCA threshold on this object.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 3-768 ThresholdCrossingAlarmSAP

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmSAP (4970) Type: thresholdCrossed Package: vpls.ThresholdCrossingAlarmSAP Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a SAP attribute crosses a TCA threshold.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 3-769 TIAESOtu15Min

Alarm	Attributes	Applicable major release
Name: TIAESOtu15Min (3482) Type: qualityOfServiceAlarm Package: equipment.TIAESOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_IAES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a IAES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-770 TIAESOtu1Day

Alarm	Attributes	Applicable major release
Name: TIAESOtu1Day (3483) Type: qualityOfServiceAlarm Package: equipment.TIAESOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_IAES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a IAES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-771 TIAESTcm15Min

Alarm	Attributes	Applicable major release
Name: TIAESTcm15Min (4585) Type: qualityOfServiceAlarm Package: equipment.TIAESTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_IAES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a IAES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-772 TIAESTcm1Day

Alarm	Attributes	Applicable major release
Name: TIAESTcm1Day (4586) Type: qualityOfServiceAlarm Package: equipment.TIAESTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_IAES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a IAES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-773 TimOduOut

Alarm	Attributes	Applicable major release
Name: TimOduOut (4597) Type: communicationsAlarm Package: equipment.TimOduOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TimOduOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing Trail Identifier Mismatch - ODU is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-774 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 3-775 ToDDEG

Alarm	Attributes	Applicable major release
Name: ToDDEG (3973) Type: communicationsAlarm Package: ptp.ToDDEG Raised on class: ptp.PTPTOD	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ToDDEG	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when ToD degrade is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-776 ToDLOS

Alarm	Attributes	Applicable major release
Name: ToDLOS (3974) Type: communicationsAlarm Package: ptp.ToDLOS Raised on class: ptp.PTPTOD	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ToDLOS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Loss of Signal is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-777 TODRefUnstable

Alarm	Attributes	Applicable major release
Name: TODRefUnstable (4957) Type: communicationsAlarm Package: ptp.TODRefUnstable Raised on class: ptp.PTPTOD	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TODRefUnstable	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the current time reference is unstable.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-778 TopologyInvalid

Alarm	Attributes	Applicable major release
Name: TopologyInvalid (4874) Type: equipmentAlarm Package: netw.TopologyInvalid Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrcdrErrTopo	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Invalid topology is detected.		
Remedial action: 1. Examine the cross-connects on the NE, and look for cross-connects that do not conform to the rules. These cross-connects are considered invalid. 2. Delete the invalid connections. Any service that is running over an invalid cross-connect that is deleted is interrupted. 3. Recreate valid cross-connects for the interrupted services.		

Table 3-779 TOprh15Min

Alarm	Attributes	Applicable major release
Name: TOprh15Min (3484) Type: qualityOfServiceAlarm Package: equipment.TOprh15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRH_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-780 TOprh1Day

Alarm	Attributes	Applicable major release
Name: TOprh1Day (3485) Type: qualityOfServiceAlarm Package: equipment.TOprh1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRH_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-781 TOprhLane1

Alarm	Attributes	Applicable major release
Name: TOprhLane1 (5451) Type: communicationsAlarm Package: equipment.TOprhLane1 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRH_LANE_1 Applicable probable causes: • T_OPRH_LANE_1 • T_OPRH_LANE_2 • T_OPRH_LANE_3 • T_OPRH_LANE_4 • T_OPRH_LANE_5 • T_OPRH_LANE_6 • T_OPRH_LANE_7 • T_OPRH_LANE_8 • T_OPRH_LANE_9 • T_OPRH_LANE_10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Network Lane1 (RX) High Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-782 TOprl15Min

Alarm	Attributes	Applicable major release
Name: TOprl15Min (3486) Type: qualityOfServiceAlarm Package: equipment.TOprl15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRL_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-783 TOprl1Day

Alarm	Attributes	Applicable major release
Name: TOprl1Day (3487) Type: qualityOfServiceAlarm Package: equipment.TOprl1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRL_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPRL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-784 TOprlLane1

Alarm	Attributes	Applicable major release
Name: TOprlLane1 (5452) Type: communicationsAlarm Package: equipment.TOprlLane1 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPRL_LANE_1 Applicable probable causes: • T_OPRL_LANE_1 • T_OPRL_LANE_2 • T_OPRL_LANE_3 • T_OPRL_LANE_4 • T_OPRL_LANE_5 • T_OPRL_LANE_6 • T_OPRL_LANE_7 • T_OPRL_LANE_8 • T_OPRL_LANE_9 • T_OPRL_LANE_10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Network Lane1 (RX) Low Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-785 TOpth15Min

Alarm	Attributes	Applicable major release
Name: TOpth15Min (3488) Type: qualityOfServiceAlarm Package: equipment.TOpth15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTH_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-786 TOpth1Day

Alarm	Attributes	Applicable major release
Name: TOpth1Day (3489) Type: qualityOfServiceAlarm Package: equipment.TOpth1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTH_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTH tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-787 TOpthLane1

Alarm	Attributes	Applicable major release
Name: TOpthLane1 (5453) Type: communicationsAlarm Package: equipment.TOpthLane1 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTH_LANE_1 Applicable probable causes: • T_OPTH_LANE_1 • T_OPTH_LANE_2 • T_OPTH_LANE_3 • T_OPTH_LANE_4 • T_OPTH_LANE_5 • T_OPTH_LANE_6 • T_OPTH_LANE_7 • T_OPTH_LANE_8 • T_OPTH_LANE_9 • T_OPTH_LANE_10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Network Lane1 (TX) High Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-788 TOptl15Min

Alarm	Attributes	Applicable major release
Name: TOptl15Min (3490) Type: qualityOfServiceAlarm Package: equipment.TOptl15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTL_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-789 TOptl1Day

Alarm	Attributes	Applicable major release
Name: TOptl1Day (3491) Type: qualityOfServiceAlarm Package: equipment.TOptl1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTL_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a OPTL tidemark Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-790 TOptlLane1

Alarm	Attributes	Applicable major release
Name: TOptlLane1 (5454) Type: communicationsAlarm Package: equipment.TOptlLane1 Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_OPTL_LANE_1 Applicable probable causes: • T_OPTL_LANE_1 • T_OPTL_LANE_2 • T_OPTL_LANE_3 • T_OPTL_LANE_4 • T_OPTL_LANE_5 • T_OPTL_LANE_6 • T_OPTL_LANE_7 • T_OPTL_LANE_8 • T_OPTL_LANE_9 • T_OPTL_LANE_10	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Network Lane1 (TX) Low Threshold Crossing detection .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-791 TPmonDmaBfd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmaBfd15Min (5511) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmaBfd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMABFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test aBfd PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-792 TPmonDmaBfd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmaBfd1Day (5512) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmaBfd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMABFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test aBfd PMON parameter for the 1Day interval.		

Table 3-792 TPmonDmaBfd1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-793 TPmonDmaffd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmaffd15Min (5515) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmaffd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMAFFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test affd PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-794 TPmonDmaffd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmaffd1Day (5516) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmaffd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMAFFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test affd PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-795 TPmonDmafFdv15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmafFdv15Min (5513) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmafFdv15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMAFFDV_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test afFdv PMON parameter for the 15Min interval.		

Table 3-795 TPmonDmafFdv15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-796 TPmonDmafFdv1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmafFdv1Day (5514) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmafFdv1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMAFFDV_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test afFdv PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-797 TPmonDmanfd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmanfd15Min (5519) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmanfd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMANFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test anfd PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-798 TPmonDmanfd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmanfd1Day (5520) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmanfd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMANFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test anfd PMON parameter for the 1Day interval.		

Table 3-798 TPmonDmanfd1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-799 TPmonDmanFdv15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmanFdv15Min (5517) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmanFdv15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMANFDV_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test anFdv PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-800 TPmonDmanFdv1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmanFdv1Day (5518) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmanFdv1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMANFDV_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test anFdv PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-801 TPmonDmxBfd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmxBfd15Min (5521) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxBfd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXBFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xBfd PMON parameter for the 15Min interval.		

Table 3-801 TPmonDmxBfd15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-802 TPmonDmxBfd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmxBfd1Day (5522) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxBfd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXBFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xBfd PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-803 TPmonDmxffd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmxffd15Min (5525) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxffd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXFFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xffd PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-804 TPmonDmxffd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmxffd1Day (5526) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxffd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXFFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xffd PMON parameter for the 1Day interval.		

Table 3-804 TPmonDmxffd1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-805 TPmonDmxfFdv15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmxfFdv15Min (5523) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxfFdv15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXFFDV_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xfFdv PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-806 TPmonDmxfFdv1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmxfFdv1Day (5524) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxfFdv1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXFFDV_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xfFdv PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-807 TPmonDmxnfd15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmxnfd15Min (5529) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxnfd15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXNFD_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xnfd PMON parameter for the 15Min interval.		

Table 3-807 TPmonDmxnfd15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-808 TPmonDmxnfd1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmxnfd1Day (5530) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxnfd1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXNFD_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xnfd PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-809 TPmonDmxnFdv15Min

Alarm	Attributes	Applicable major release
Name: TPmonDmxnFdv15Min (5527) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxnFdv15Min Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXNFDV_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xnFdv PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-810 TPmonDmxnFdv1Day

Alarm	Attributes	Applicable major release
Name: TPmonDmxnFdv1Day (5528) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonDmxnFdv1Day Raised on class: ethernetoam.CfmTwoWayDelayTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_DMXNFDV_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the DM test xnFdv PMON parameter for the 1Day interval.		

Table 3-810 TPmonDmxnFdv1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-811 TPmonLmafflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmafflr15Min (5531) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmafflr15Min Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMAFFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test afFlr PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-812 TPmonLmafflr1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmafflr1Day (5532) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmafflr1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMAFFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test afFlr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-813 TPmonLmanflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmanflr15Min (5533) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmanflr15Min Raised on class: ethernetoam.CfmLMTest	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMANFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test anflr PMON parameter for the 15Min interval.		

Table 3-813 TPmonLmanflr15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-814 TPmonLmanflr1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmanflr1Day (5534) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmanflr1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMANFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test anflr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-815 TPmonLmfhli15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmfhli15Min (5535) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmfhli15Min Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMFHLI_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test fhli PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-816 TPmonLmfhli1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmfhli1Day (5536) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmfhli1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMFHLI_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test fhli PMON parameter for the 1Day interval.		

Table 3-816 TPmonLmfhli1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-817 TPmonLmnhli15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmnhli15Min (5537) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmnhli15Min Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMNHLI_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test nhli PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-818 TPmonLmnhli1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmnhli1Day (5538) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmnhli1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMNHLI_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test nhli PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-819 TPmonLmxfflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmxfflr15Min (5539) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmxfflr15Min Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMXFFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test xfFlr PMON parameter for the 15Min interval.		

Table 3-819 TPmonLmxfflr15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-820 TPmonLmxfflr1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmxfflr1Day (5540) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmxfflr1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMXFFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test xfFlr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-821 TPmonLmxnflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonLmxnflr15Min (5541) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmxnflr15Min Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMXNFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test xnFlr PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-822 TPmonLmxnflr1Day

Alarm	Attributes	Applicable major release
Name: TPmonLmxnflr1Day (5542) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonLmxnflr1Day Raised on class: ethernetoam.CfmLMTest	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_LMXNFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the LM test xnFlr PMON parameter for the 1Day interval.		

Table 3-822 TPmonLmxnflr1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-823 TPmonPortHighCapacityOctets15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortHighCapacityOctets15Min (5455) Type: qualityOfServiceAlarm Package: equipment. TPmonPortHighCapacityOctets15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTHIGHCAPACITYOCTETS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port HighCapacityOctets PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-824 TPmonPortHighCapacityOctets1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortHighCapacityOctets1Day (5456) Type: qualityOfServiceAlarm Package: equipment. TPmonPortHighCapacityOctets1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTHIGHCAPACITYOCTETS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port HighCapacityOctets PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-825 TPmonPortHighCapacityPkts15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortHighCapacityPkts15Min (5457) Type: qualityOfServiceAlarm Package: equipment. TPmonPortHighCapacityPkts15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTHIGHCAPACITYPKTS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port HighCapacityPkts PMON parameter for the 15Min interval.		

Table 3-825 TPmonPortHighCapacityPkts15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-826 TPmonPortHighCapacityPkts1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortHighCapacityPkts1Day (5458) Type: qualityOfServiceAlarm Package: equipment. TPmonPortHighCapacityPkts1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTHIGHCAPACITYPKTS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port HighCapacityPkts PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-827 TPmonPortIfInDiscards15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInDiscards15Min (5459) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInDiscards15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINDISCARDS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInDiscards PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-828 TPmonPortIfInDiscards1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInDiscards1Day (5460) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInDiscards1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINDISCARDS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInDiscards PMON parameter for the 1Day interval.		

Table 3-828 TPmonPortIfInDiscards1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-829 TPmonPortIfInErrors15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInErrors15Min (5461) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInErrors15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINERRORS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInErrors PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-830 TPmonPortIfInErrors1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInErrors1Day (5462) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInErrors1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINERRORS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInErrors PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-831 TPmonPortIfInOctets15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInOctets15Min (5463) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInOctets15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINOCTETS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInOctets PMON parameter for the 15Min interval.		

Table 3-831 TPmonPortIfInOctets15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-832 TPmonPortIfInOctets1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInOctets1Day (5464) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInOctets1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINOCTETS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInOctets PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-833 TPmonPortIfInPackets15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInPackets15Min (5465) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInPackets15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINPACKETS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInPackets PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-834 TPmonPortIfInPackets1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfInPackets1Day (5466) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfInPackets1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFINPACKETS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfInPackets PMON parameter for the 1Day interval.		

Table 3-834 TPmonPortIfInPackets1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-835 TPmonPortIfOutDiscards15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutDiscards15Min (5467) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutDiscards15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTDISCARDS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutDiscards PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-836 TPmonPortIfOutDiscards1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutDiscards1Day (5468) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutDiscards1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTDISCARDS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutDiscards PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-837 TPmonPortIfOutErrors15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutErrors15Min (5469) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutErrors15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTERRORS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutErrors PMON parameter for the 15Min interval.		

Table 3-837 TPmonPortIfOutErrors15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-838 TPmonPortIfOutErrors1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutErrors1Day (5470) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutErrors1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTERRORS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutErrors PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-839 TPmonPortIfOutOctets15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutOctets15Min (5471) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutOctets15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTOCTETS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutOctets PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-840 TPmonPortIfOutOctets1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutOctets1Day (5472) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutOctets1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTOCTETS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutOctets PMON parameter for the 1Day interval.		

Table 3-840 TPmonPortIfOutOctets1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-841 TPmonPortIfOutPackets15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutPackets15Min (5473) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutPackets15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTPACKETS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutPackets PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-842 TPmonPortIfOutPackets1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortIfOutPackets1Day (5474) Type: qualityOfServiceAlarm Package: equipment.TPmonPortIfOutPackets1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTIFOUTPACKETS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port IfOutPackets PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-843 TPmonPortQueue1OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue1OctetsDropped15Min (5475) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue1OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE1OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 1 Octets dropped PMON parameter for the 15Min interval.		

Table 3-843 TPmonPortQueue1OctetsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-844 TPmonPortQueue1OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue1OctetsDropped1Day (5476) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue1OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 1 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-845 TPmonPortQueue1PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue1PktsDropped15Min (5477) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue1PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE1PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 1 Packets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-846 TPmonPortQueue1PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue1PktsDropped1Day (5478) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue1PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 1 Packets dropped PMON parameter for the 1Day interval.		

Table 3-846 TPmonPortQueue1PktsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-847 TPmonPortQueue2OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue2OctetsDropped15Min (5479) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue2OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE2OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 2 Octets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-848 TPmonPortQueue2OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue2OctetsDropped1Day (5480) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue2OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 2 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-849 TPmonPortQueue2PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue2PktsDropped15Min (5481) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue2PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE2PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 2 Packets dropped PMON parameter for the 15Min interval.		

Table 3-849 TPmonPortQueue2PktsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-850 TPmonPortQueue2PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue2PktsDropped1Day (5482) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue2PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 2 Packets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-851 TPmonPortQueue3OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue3OctetsDropped15Min (5483) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue3OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUE3OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 3 Octets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-852 TPmonPortQueue3OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue3OctetsDropped1Day (5484) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue3OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 3 Octets dropped PMON parameter for the 1Day interval.		

Table 3-852 TPmonPortQueue3OctetsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-853 TPmonPortQueue3PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue3PktsDropped15Min (5485) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue3PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUE3PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 3 Packets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-854 TPmonPortQueue3PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue3PktsDropped1Day (5486) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue3PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 3 Packets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-855 TPmonPortQueue4OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue4OctetsDropped15Min (5487) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue4OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUE4OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 4 Octets dropped PMON parameter for the 15Min interval.		

Table 3-855 TPmonPortQueue4OctetsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-856 TPmonPortQueue4OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue4OctetsDropped1Day (5488) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue4OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 4 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-857 TPmonPortQueue4PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue4PktsDropped15Min (5489) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue4PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE4PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 4 Packets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-858 TPmonPortQueue4PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue4PktsDropped1Day (5490) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue4PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 4 Packets dropped PMON parameter for the 1Day interval.		

Table 3-858 TPmonPortQueue4PktsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-859 TPmonPortQueue5OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue5OctetsDropped15Min (5491) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue5OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE5OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 5 Octets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-860 TPmonPortQueue5OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue5OctetsDropped1Day (5492) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue5OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 5 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-861 TPmonPortQueue5PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue5PktsDropped15Min (5493) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue5PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE5PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 5 Packets dropped PMON parameter for the 15Min interval.		

Table 3-861 TPmonPortQueue5PktsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-862 TPmonPortQueue5PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue5PktsDropped1Day (5494) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue5PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 5 Packets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-863 TPmonPortQueue6OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue6OctetsDropped15Min (5495) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue6OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUE6OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 6 Octets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-864 TPmonPortQueue6OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue6OctetsDropped1Day (5496) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue6OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 6 Octets dropped PMON parameter for the 1Day interval.		

Table 3-864 TPmonPortQueue6OctetsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-865 TPmonPortQueue6PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue6PktsDropped15Min (5497) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue6PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE6PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 6 Packets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-866 TPmonPortQueue6PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue6PktsDropped1Day (5498) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue6PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 6 Packets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-867 TPmonPortQueue7OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue7OctetsDropped15Min (5499) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue7OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE7OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 7 Octets dropped PMON parameter for the 15Min interval.		

Table 3-867 TPmonPortQueue7OctetsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-868 TPmonPortQueue7OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue7OctetsDropped1Day (5500) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue7OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 7 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-869 TPmonPortQueue7PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue7PktsDropped15Min (5501) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue7PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE7PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 7 Packets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-870 TPmonPortQueue7PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue7PktsDropped1Day (5502) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue7PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 7 Packets dropped PMON parameter for the 1Day interval.		

Table 3-870 TPmonPortQueue7PktsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-871 TPmonPortQueue8OctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue8OctetsDropped15Min (5503) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue8OctetsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE8OCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 8 Octets dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-872 TPmonPortQueue8OctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue8OctetsDropped1Day (5504) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue8OctetsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUEOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 8 Octets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-873 TPmonPortQueue8PktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue8PktsDropped15Min (5505) Type: qualityOfServiceAlarm Package: equipment. TPmonPortQueue8PktsDropped15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ PORTQUEUE8PKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 8 Packets dropped PMON parameter for the 15Min interval.		

Table 3-873 TPmonPortQueue8PktsDropped15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-874 TPmonPortQueue8PktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonPortQueue8PktsDropped1Day (5506) Type: qualityOfServiceAlarm Package: equipment.TPmonPortQueue8PktsDropped1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_PORTQUEUEPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the Port Queue 8 Packets dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-875 TPmonSapIngressOctetsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonSapIngressOctetsDropped15Min (5598) Type: qualityOfServiceAlarm Package: vpls.TPmonSapIngressOctetsDropped15Min Raised on class: vpls.L2AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ SAPINGRESSOCTETSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the SAP Ingress Octets Dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-876 TPmonSapIngressOctetsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonSapIngressOctetsDropped1Day (5599) Type: qualityOfServiceAlarm Package: vpls.TPmonSapIngressOctetsDropped1Day Raised on class: vpls.L2AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ SAPINGRESSOCTETSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the SAP Ingress Octets Dropped PMON parameter for the 1Day interval.		

Table 3-876 TPmonSapIngressOctetsDropped1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-877 TPmonSapIngressPktsDropped15Min

Alarm	Attributes	Applicable major release
Name: TPmonSapIngressPktsDropped15Min (5600) Type: qualityOfServiceAlarm Package: vpls.TPmonSapIngressPktsDropped15Min Raised on class: vpls.L2AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ SAPINGRESSPKTSDROPPED_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the SAP Ingress Packets Dropped PMON parameter for the 15Min interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-878 TPmonSapIngressPktsDropped1Day

Alarm	Attributes	Applicable major release
Name: TPmonSapIngressPktsDropped1Day (5601) Type: qualityOfServiceAlarm Package: vpls.TPmonSapIngressPktsDropped1Day Raised on class: vpls.L2AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_ SAPINGRESSPKTSDROPPED_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Threshold Crossing Alert has been detected for the SAP Ingress Packets Dropped PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-879 TPmonSlmafflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonSlmafflr15Min (5544) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmafflr15Min Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMAFFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test afflr PMON parameter for the 15Min interval.		

Table 3-879 TPmonSlmafflr15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-880 TPmonSlmafFlr1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmafFlr1Day (5543) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmafFlr1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMAFFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test afFlr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-881 TPmonSlmafflrContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmafflrContinuous (5545) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmafflrContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMAFFLR_CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test afflr PMON parameter - continuous.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-882 TPmonSlmanflr15Min

Alarm	Attributes	Applicable major release
Name: TPmonSlmanflr15Min (5547) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmanflr15Min Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMANFLR_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test anflr PMON parameter for the 15Min interval.		

Table 3-882 TPmonSlmanflr15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-883 TPmonSlmanFlr1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmanFlr1Day (5546) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmanFlr1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMANFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test anFlr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-884 TPmonSlmanflrContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmanflrContinuous (5548) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmanflrContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMANFLR_CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test anflr PMON parameter - continuous.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-885 TPmonSlmfhli15Min

Alarm	Attributes	Applicable major release
Name: TPmonSlmfhli15Min (5549) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmfhli15Min Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMFHLI_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test fhli PMON parameter for the 15Min interval.		

Table 3-885 TPmonSlmfhli15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-886 TPmonSlmfhli1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmfhli1Day (5550) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmfhli1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMFHLI_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test fhli PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-887 TPmonSlmfhliContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmfhliContinuous (5551) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmfhliContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMFHLI_CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test fhli PMON parameter - continuous.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-888 TPmonSlmnhli15Min

Alarm	Attributes	Applicable major release
Name: TPmonSlmnhli15Min (5552) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmnhli15Min Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMNHLI_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test nhli PMON parameter for the 15Min interval.		

Table 3-888 TPmonSlmnhli15Min (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-889 TPmonSlmnhli1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmnhli1Day (5553) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmnhli1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMNHLI_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test nhli PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-890 TPmonSlmnhliContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmnhliContinuous (5554) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmnhliContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMNHLI_ CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test nhli PMON parameter - continuous.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-891 TPmonSlmxfFlr1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmxfFlr1Day (5555) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmxfFlr1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMXFFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test xfFlr PMON parameter for the 1Day interval.		

Table 3-891 TPmonSlmxfFlr1Day (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-892 TPmonSlmxfflrContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmxfflrContinuous (5556) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmxfflrContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMXFFLR_CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test xfflr PMON parameter - continuous.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-893 TPmonSlmxnFlr1Day

Alarm	Attributes	Applicable major release
Name: TPmonSlmxnFlr1Day (5557) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmxnFlr1Day Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMXNFLR_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test xnFlr PMON parameter for the 1Day interval.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-894 TPmonSlmxnflrContinuous

Alarm	Attributes	Applicable major release
Name: TPmonSlmxnflrContinuous (5558) Type: qualityOfServiceAlarm Package: ethernetoam.TPmonSlmxnflrContinuous Raised on class: ethernetoam.CfmTwoWaySlm	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PMON_SLMXNFLR_ CONTINUOUS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a Threshold Crossing Alert has been detected for the SLM test nflr PMON parameter - continuous.		

Table 3-894 TPmonSlmxnflrContinuous (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-895 TPostfec15Min

Alarm	Attributes	Applicable major release
Name: TPostfec15Min (3492) Type: qualityOfServiceAlarm Package: equipment.TPostfec15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_POSTFEC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Post-FEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-896 TPostfec1Day

Alarm	Attributes	Applicable major release
Name: TPostfec1Day (3493) Type: qualityOfServiceAlarm Package: equipment.TPostfec1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_POSTFEC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Post-FEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-897 TPrefec15Min

Alarm	Attributes	Applicable major release
Name: TPrefec15Min (3494) Type: qualityOfServiceAlarm Package: equipment.TPrefec15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PREFEC_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Pre-FEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-898 TPrefec1Day

Alarm	Attributes	Applicable major release
Name: TPrefec1Day (3495) Type: qualityOfServiceAlarm Package: equipment.TPrefec1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_PREFEC_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a Pre-FEC BER Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-899 TrailTraceIdentifierMismatch

Alarm	Attributes	Applicable major release
Name: TrailTraceIdentifierMismatch (4598) Type: communicationsAlarm Package: equipment.TrailTraceIdentifierMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Tim Applicable probable causes: • Tim • TimOdu • TrailTraceIdentifierMismatchEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trail Identifier Mismatch - OTU is detected.		
Remedial action: This alarm is raised when the incoming optical channel trail trace message does not match the expected incoming optical channel trail trace message.Refer TIMODU (Trace Identifier Mismatch - ODU) in 1830 Troubleshooting guide for detailed corrective procedure.		

Table 3-900 TrailTraceIdentifierMismatchEgress

Alarm	Attributes	Applicable major release
Name: TrailTraceIdentifierMismatchEgress (4940) Type: communicationsAlarm Package: equipment.TrailTraceIdentifierMismatchEgress Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TrailTraceIdentifierMismatchEgress	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Trail Identifier Mismatch Egress - ODU .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-901 TransferLogFL

Alarm	Attributes	Applicable major release
Name: TransferLogFL (4875) Type: communicationsAlarm Package: netw.TransferLogFL Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TransferLogFL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when transfer log Failtemp file read or create fail is detected.		
Remedial action: 1.Retry transfer again. 2. If problem persists, contact your Nokia support representative for assistance.		

Table 3-902 TransferLogFT

Alarm	Attributes	Applicable major release
Name: TransferLogFT (4876) Type: communicationsAlarm Package: netw.TransferLogFT Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TransferLogFT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when transfer log fail is detected.		
Remedial action: 1.Retry transfer again. 2. If problem persists, contact your Nokia support representative for assistance.		

Table 3-903 TransferLogIP

Alarm	Attributes	Applicable major release
Name: TransferLogIP (4877) Type: communicationsAlarm Package: netw.TransferLogIP Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TransferLogIP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when transfer log in progress is detected.		
Remedial action: No corrective action is required. The alarm clears automatically when the log file transfer has completed successfully or failed.		

Table 3-904 TransmitLaserOffRxFaultDuringLineLoopback

Alarm	Attributes	Applicable major release
Name: TransmitLaserOffRxFaultDuringLineLoopback (2107) Type: communicationsAlarm Package: equipment.TransmitLaserOffRxFaultDuringLineLoopback Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LaserOffLpbk	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Transmit laser off - rx fault during line loopback is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-905 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		

Table 3-905 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 3-906 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		

Table 3-906 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 3-907 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 3-908 TrmtMOD

Alarm	Attributes	Applicable major release
Name: TrmtMOD (3546) Type: equipmentAlarm Package: equipment.TrmtMOD Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TrmtMOD	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Pluggable Module transmit failure is detected.		
Remedial action: This alarm is raised at the pluggable module equipment and indicates a fault on the transmit port of the pluggable module. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Perform a warm reset of the card.\n 2. Remove the pluggable module from the port on the card it is inserted in. Examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage. If no damage is seen, reinsert the pluggable module into its port.\n 3. Remove and replace the pluggable module with another unit of the same type.\n 4. Perform a cold reset of the card.\n 5. Reseat the card.\n 6. Replace the card.\n For Detailed steps Please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-909 TRUBRKROPEN

Alarm	Attributes	Applicable major release
Name: TRUBRKROPEN (4938) Type: communicationsAlarm Package: equipment.TRUBRKROPEN Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TRUBRKROPEN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0

Table 3-909 TRUBRKROPEN (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Open circuit breaker .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-910 TRUSVCVOLTFLT

Alarm	Attributes	Applicable major release
Name: TRUSVCVOLTFLT (4939) Type: communicationsAlarm Package: equipment.TRUSVCVOLTFLT Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TRUSVCVOLTFLT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bad Service Voltage on OneTRU Alarm Board .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-911 TSefs15Min

Alarm	Attributes	Applicable major release
Name: TSefs15Min (3496) Type: qualityOfServiceAlarm Package: equipment.TSefs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-912 TSefs1Day

Alarm	Attributes	Applicable major release
Name: TSefs1Day (3497) Type: qualityOfServiceAlarm Package: equipment.TSefs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-913 TSefsPcs15Min

Alarm	Attributes	Applicable major release
Name: TSefsPcs15Min (3498) Type: qualityOfServiceAlarm Package: equipment.TSefsPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-914 TSefsPcs1Day

Alarm	Attributes	Applicable major release
Name: TSefsPcs1Day (3499) Type: qualityOfServiceAlarm Package: equipment.TSefsPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-915 TSefsPcst15Min

Alarm	Attributes	Applicable major release
Name: TSefsPcst15Min (3500) Type: qualityOfServiceAlarm Package: equipment.TSefsPcst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-916 TSefsPcst1Day

Alarm	Attributes	Applicable major release
Name: TSefsPcst1Day (3501) Type: qualityOfServiceAlarm Package: equipment.TSefsPcst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-917 TSefss15Min

Alarm	Attributes	Applicable major release
Name: TSefss15Min (3502) Type: qualityOfServiceAlarm Package: equipment.TSefss15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFSS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-918 TSefss1Day

Alarm	Attributes	Applicable major release
Name: TSefss1Day (3503) Type: qualityOfServiceAlarm Package: equipment.TSefss1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFSS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-919 TSefsst15Min

Alarm	Attributes	Applicable major release
Name: TSefsst15Min (3504) Type: qualityOfServiceAlarm Package: equipment.TSefsst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFSST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-920 TSefsst1Day

Alarm	Attributes	Applicable major release
Name: TSefsst1Day (3505) Type: qualityOfServiceAlarm Package: equipment.TSefsst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFSST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SEFS-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-921 TSes15Min

Alarm	Attributes	Applicable major release
Name: TSes15Min (3506) Type: qualityOfServiceAlarm Package: equipment.TSes15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-922 TSes1Day

Alarm	Attributes	Applicable major release
Name: TSes1Day (3507) Type: qualityOfServiceAlarm Package: equipment.TSes1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-923 TSesL15Min

Alarm	Attributes	Applicable major release
Name: TSesL15Min (3508) Type: qualityOfServiceAlarm Package: equipment.TSesL15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_L_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-L Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-924 TSesL1Day

Alarm	Attributes	Applicable major release
Name: TSesL1Day (3509) Type: qualityOfServiceAlarm Package: equipment.TSesL1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_L_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-L Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-925 TSesMs15Min

Alarm	Attributes	Applicable major release
Name: TSesMs15Min (3510) Type: qualityOfServiceAlarm Package: equipment.TSesMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-926 TSesMs1Day

Alarm	Attributes	Applicable major release
Name: TSesMs1Day (3511) Type: qualityOfServiceAlarm Package: equipment.TSesMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-927 TSesOdu15Min

Alarm	Attributes	Applicable major release
Name: TSesOdu15Min (3512) Type: qualityOfServiceAlarm Package: equipment.TSesOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-928 TSesOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TSesOdu15MinOut (8458) Type: qualityOfServiceAlarm Package: equipment.TSesOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-929 TSesOdu1Day

Alarm	Attributes	Applicable major release
Name: TSesOdu1Day (3513) Type: qualityOfServiceAlarm Package: equipment.TSesOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-930 TSesOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TSesOdu1DayOut (8459) Type: qualityOfServiceAlarm Package: equipment.TSesOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-931 TSesOtu15Min

Alarm	Attributes	Applicable major release
Name: TSesOtu15Min (3514) Type: qualityOfServiceAlarm Package: equipment.TSesOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-932 TSesOtu1Day

Alarm	Attributes	Applicable major release
Name: TSesOtu1Day (3515) Type: qualityOfServiceAlarm Package: equipment.TSesOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-933 TSesP15Min

Alarm	Attributes	Applicable major release
Name: TSesP15Min (3516) Type: qualityOfServiceAlarm Package: equipment.TSesP15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_P_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-934 TSesP1Day

Alarm	Attributes	Applicable major release
Name: TSesP1Day (3517) Type: qualityOfServiceAlarm Package: equipment.TSesP1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_P_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-935 TSesPcs15Min

Alarm	Attributes	Applicable major release
Name: TSesPcs15Min (3518) Type: qualityOfServiceAlarm Package: equipment.TSesPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-936 TSesPcs1Day

Alarm	Attributes	Applicable major release
Name: TSesPcs1Day (3519) Type: qualityOfServiceAlarm Package: equipment.TSesPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-937 TSesPcst15Min

Alarm	Attributes	Applicable major release
Name: TSesPcst15Min (3520) Type: qualityOfServiceAlarm Package: equipment.TSesPcst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-938 TSesPcst1Day

Alarm	Attributes	Applicable major release
Name: TSesPcst1Day (3521) Type: qualityOfServiceAlarm Package: equipment.TSesPcst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-939 TSesPt15Min

Alarm	Attributes	Applicable major release
Name: TSesPt15Min (3522) Type: qualityOfServiceAlarm Package: equipment.TSesPt15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-940 TSesPt1Day

Alarm	Attributes	Applicable major release
Name: TSesPt1Day (3523) Type: qualityOfServiceAlarm Package: equipment.TSesPt1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-941 TSesRs15Min

Alarm	Attributes	Applicable major release
Name: TSesRs15Min (3524) Type: qualityOfServiceAlarm Package: equipment.TSesRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-942 TSesRs1Day

Alarm	Attributes	Applicable major release
Name: TSesRs1Day (3525) Type: qualityOfServiceAlarm Package: equipment.TSesRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-943 TSesRst15Min

Alarm	Attributes	Applicable major release
Name: TSesRst15Min (3526) Type: qualityOfServiceAlarm Package: equipment.TSesRst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-944 TSesRst1Day

Alarm	Attributes	Applicable major release
Name: TSesRst1Day (3527) Type: qualityOfServiceAlarm Package: equipment.TSesRst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_RST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-945 TSess15Min

Alarm	Attributes	Applicable major release
Name: TSess15Min (3528) Type: qualityOfServiceAlarm Package: equipment.TSess15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SESS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-946 TSess1Day

Alarm	Attributes	Applicable major release
Name: TSess1Day (3529) Type: qualityOfServiceAlarm Package: equipment.TSess1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SESS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-947 TSesst15Min

Alarm	Attributes	Applicable major release
Name: TSesst15Min (3530) Type: qualityOfServiceAlarm Package: equipment.TSesst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SESST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-948 TSesst1Day

Alarm	Attributes	Applicable major release
Name: TSesst1Day (3531) Type: qualityOfServiceAlarm Package: equipment.TSesst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SESST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-S Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-949 TSesTcm15Min

Alarm	Attributes	Applicable major release
Name: TSesTcm15Min (4587) Type: qualityOfServiceAlarm Package: equipment.TSesTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-950 TSesTcm1Day

Alarm	Attributes	Applicable major release
Name: TSesTcm1Day (4588) Type: qualityOfServiceAlarm Package: equipment.TSesTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a SES-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-951 TsMismatch

Alarm	Attributes	Applicable major release
Name: TsMismatch (4599) Type: communicationsAlarm Package: equipment.TsMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TsMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Time Slot Assignment Mismatch is detected.		
Remedial action: 1 Check that the Client port on the Far End and Near End both have the same time slots.For CLI config interface cardname sh/sl/pt signal_rate timeslot For WEBUI On the Far End NE, Select the slot and client port of the card.Click the Time Slot tab.Select/de-select the appropriate time slots to match those selected on the Near End NE, and click Submit.		

Table 3-952 TsMismatchOut

Alarm	Attributes	Applicable major release
Name: TsMismatchOut (4600) Type: communicationsAlarm Package: equipment.TsMismatchOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TsMismatchOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Time Slot Assignment Mismatch OUT is detected.		

Table 3-952 TsMismatchOut (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1 Check that the Client port on the Far End and Near End both have the same time slots.For CLI config interface cardname sh/sl/pt signal_rate timeslot For WEBUI On the Far End NE, Select the slot and client port of the card.Click the Time Slot tab.Select/de-select the appropriate time slots to match those selected on the Near End NE, and click Submit.		

Table 3-953 TUasMs15Min

Alarm	Attributes	Applicable major release
Name: TUasMs15Min (3532) Type: qualityOfServiceAlarm Package: equipment.TUasMs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_MS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-954 TUasMs1Day

Alarm	Attributes	Applicable major release
Name: TUasMs1Day (3533) Type: qualityOfServiceAlarm Package: equipment.TUasMs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_MS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-MS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-955 TUasOdu15Min

Alarm	Attributes	Applicable major release
Name: TUasOdu15Min (3534) Type: qualityOfServiceAlarm Package: equipment.TUasOdu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-956 TUasOdu15MinOut

Alarm	Attributes	Applicable major release
Name: TUasOdu15MinOut (8460) Type: qualityOfServiceAlarm Package: equipment.TUasOdu15MinOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_15MIN_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-957 TUasOdu1Day

Alarm	Attributes	Applicable major release
Name: TUasOdu1Day (3535) Type: qualityOfServiceAlarm Package: equipment.TUasOdu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-958 TUasOdu1DayOut

Alarm	Attributes	Applicable major release
Name: TUasOdu1DayOut (8461) Type: qualityOfServiceAlarm Package: equipment.TUasOdu1DayOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_ODU_1DAY_OUT	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-ODU-OUT Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-959 TUasOtu15Min

Alarm	Attributes	Applicable major release
Name: TUasOtu15Min (3536) Type: qualityOfServiceAlarm Package: equipment.TUasOtu15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_OTU_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-960 TUasOtu1Day

Alarm	Attributes	Applicable major release
Name: TUasOtu1Day (3537) Type: qualityOfServiceAlarm Package: equipment.TUasOtu1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_OTU_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-OTU Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-961 TUasP15Min

Alarm	Attributes	Applicable major release
Name: TUasP15Min (3538) Type: qualityOfServiceAlarm Package: equipment.TUasP15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_P_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-962 TUasP1Day

Alarm	Attributes	Applicable major release
Name: TUasP1Day (3539) Type: qualityOfServiceAlarm Package: equipment.TUasP1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_P_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-P Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-963 TUasPt15Min

Alarm	Attributes	Applicable major release
Name: TUasPt15Min (3540) Type: qualityOfServiceAlarm Package: equipment.TUasPt15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_PT_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-964 TUasPt1Day

Alarm	Attributes	Applicable major release
Name: TUasPt1Day (3541) Type: qualityOfServiceAlarm Package: equipment.TUasPt1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_PT_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-PT Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-965 TUasRs15Min

Alarm	Attributes	Applicable major release
Name: TUasRs15Min (3542) Type: qualityOfServiceAlarm Package: equipment.TUasRs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RS_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-966 TUasRs1Day

Alarm	Attributes	Applicable major release
Name: TUasRs1Day (3543) Type: qualityOfServiceAlarm Package: equipment.TUasRs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RS_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-967 TUasRst15Min

Alarm	Attributes	Applicable major release
Name: TUasRst15Min (3544) Type: qualityOfServiceAlarm Package: equipment.TUasRst15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RST_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-968 TUasRst1Day

Alarm	Attributes	Applicable major release
Name: TUasRst1Day (3545) Type: qualityOfServiceAlarm Package: equipment.TUasRst1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_RST_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates a UAS-RS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 3-969 TUasTcm15Min

Alarm	Attributes	Applicable major release
Name: TUasTcm15Min (4589) Type: qualityOfServiceAlarm Package: equipment.TUasTcm15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_TCM_15MIN	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates an UAS-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-970 TUasTcm1Day

Alarm	Attributes	Applicable major release
Name: TUasTcm1Day (4590) Type: qualityOfServiceAlarm Package: equipment.TUasTcm1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_UAS_TCM_1DAY	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Indicates an UAS-ODU-TCM NearEnd Threshold Crossing detection is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-971 TunableLaserNotProvisioned

Alarm	Attributes	Applicable major release
Name: TunableLaserNotProvisioned (2108) Type: equipmentAlarm Package: equipment.TunableLaserNotProvisioned Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrcdrErr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Tunable laser not provisioned is detected.		
Remedial action: Please refer section PRCDRERR in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-972 UnexpectedWaveKey

Alarm	Attributes	Applicable major release
Name: UnexpectedWaveKey (4601) Type: communicationsAlarm Package: equipment.UnexpectedWaveKey Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchUnknown Applicable probable causes: • OchUnknown • OchUnknownOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel unexpected is detected.		
Remedial action: Please refer OCHUNKNOWN (Channel Unexpected) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-973 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		

Table 3-973 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 3-974 UnitNotInserted

Alarm	Attributes	Applicable major release
Name: UnitNotInserted (4966) Type: equipmentAlarm Package: rmd.UnitNotInserted Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfUNI	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the unit is not inserted in a RMD device of type cEDD. Applicable to customer ports only.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-975 UnknownWaveKeyForConnection

Alarm	Attributes	Applicable major release
Name: UnknownWaveKeyForConnection (4602) Type: communicationsAlarm Package: equipment.UnknownWaveKeyForConnection Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchTrailUnknown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Unknown OCH Trail for x-connect is detected.		
Remedial action: Please refer section OCHTRAILUNKNOWN (Unknown OCH Trail for x-connect) in 1830 Troubleshooting guide for detailed corrective action.		

Table 3-976 UNL

Alarm	Attributes	Applicable major release
Name: UNL (3975) Type: oamAlarm Package: ethernetoam.UNL Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UNL	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a first CCM frame is received with incorrect MEG level.		
Remedial action: This alarm is raised when a MEP receives a first CCM frame with an incorrect MEG level.		

Table 3-977 UNM

Alarm	Attributes	Applicable major release
Name: UNM (3976) Type: oamAlarm Package: ethernetoam.UNM Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UNM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives a CCM frame with a correct MEG level or MEG ID, but unexpected MEP ID which includes the MEP's own MEP ID.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an unexpected MEP ID.		

Table 3-978 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		

Table 3-978 UnmanageFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 3-979 UnMOrUnP

Alarm	Attributes	Applicable major release
Name: UnMOrUnP (3737) Type: communicationsAlarm Package: equipment.UnMOrUnP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnMOrUnP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Unexpected MEP id or periodicity is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-980 UNP

Alarm	Attributes	Applicable major release
Name: UNP (3977) Type: oamAlarm Package: ethernetoam.UNP Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UNP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives a CCM frame with a correct MEG level, a correct MEG ID, or a correct MEP ID, but with period field value different than MEP's own CCM transmission period.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with period field value different than the MEP's own CCM transmission period.		

Table 3-981 UNPr

Alarm	Attributes	Applicable major release
Name: UNPr (3978) Type: oamAlarm Package: ethernetoam.UNPr Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UNPr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a MEP receives a CCM frame with a correct MEG level, a correct MEG ID, or a correct MEP ID, but with priority field value different than MEP's own CCM transmission priority.		

Table 3-981 UNPr (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when a MEP receives a CCM frame with priority field value different than the MEP's own CCM transmission priority.		

Table 3-982 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 3-983 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 3-984 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all connections of the Uplink are down.		

Table 3-984 UplinkDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 3-985 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 3-986 UruO

Alarm	Attributes	Applicable major release
Name: UruO (9051) Type: communicationsAlarm Package: equipment.UruO Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruO	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - port .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-987 UruOchLos

Alarm	Attributes	Applicable major release
Name: UruOchLos (3547) Type: communicationsAlarm Package: equipment.UruOchLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOchLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - OCH-LOS is detected.		
Remedial action: Perform corrective action as described in LOS - Loss of Signal		

Table 3-988 UruOmsRx

Alarm	Attributes	Applicable major release
Name: UruOmsRx (3548) Type: communicationsAlarm Package: equipment.UruOmsRx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOmsRx	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - OMS-RX is detected.		
Remedial action: This alarm indicates that there is an active LOSCWRSIG alarm at the Sig In port of an CWR8, CWR8-88 or WR8-88 card.\n For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-989 UruOmsTx

Alarm	Attributes	Applicable major release
Name: UruOmsTx (3920) Type: communicationsAlarm Package: equipment.UruOmsTx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOmsTx	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - OMS-TX is detected.		
Remedial action: Informational - no corrective action required.		

Table 3-990 UruOtsLos

Alarm	Attributes	Applicable major release
Name: UruOtsLos (3549) Type: communicationsAlarm Package: equipment.UruOtsLos Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOtsLos	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying Resource unavailable - OTS-LOS is detected.		
Remedial action: For corrective action please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-991 UruOtsRx

Alarm	Attributes	Applicable major release
Name: UruOtsRx (3550) Type: communicationsAlarm Package: equipment.UruOtsRx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOtsRx	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - OTS-RX is detected.		
Remedial action: Please follow the below steps to clear this alarm:\n 1. Retrieve the list of current alarms and conditions on the network element.\n 2. Perform corrective action as described in the appropriate LOS alarm trouble-clearing procedure at the alarmed port other than the network facing LINE/LINEIN port.		

Table 3-992 UruOtsTx

Alarm	Attributes	Applicable major release
Name: UruOtsTx (3551) Type: communicationsAlarm Package: equipment.UruOtsTx Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOtsTx	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - OTS-TX is detected.		
Remedial action: Please follow the below steps to clear this alarm:\n 1. Retrieve the list of current alarms and conditions on the network element.\n 2. Perform corrective action as described in the appropriate LOS alarm trouble-clearing procedure at the alarmed port other than the network facing LINE/LINEIN port.		

Table 3-993 UruOtu

Alarm	Attributes	Applicable major release
Name: UruOtu (3552) Type: communicationsAlarm Package: equipment.UruOtu Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruOtu	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - port is detected.		
Remedial action: Perform corrective action as described in LOS - Loss of Signal at the LINE/LINEIN port.		

Table 3-994 UruP

Alarm	Attributes	Applicable major release
Name: UruP (9052) Type: communicationsAlarm Package: equipment.UruP Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - Path .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-995 UruS

Alarm	Attributes	Applicable major release
Name: UruS (3553) Type: communicationsAlarm Package: equipment.UruS Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UruS	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Underlying resource unavailable - card is detected.		
Remedial action: This alarm indicates that an I/O card or server card has failed, and as a result one or more OTU port are affected. Please follow the below steps to clear this alarm:\n 1. According to your needs,\n a. delete(deprovision) the I/O card.\n b. insert the correct I/O card into the slot.\n c. replace the respective failed I/O card.\n 2. Refresh the list of current alarms, if the alarm persist contact your Nokia support representative for assistance.		

Table 3-996 UserEqptMismatch

Alarm	Attributes	Applicable major release
Name: UserEqptMismatch (4603) Type: equipmentAlarm Package: equipment.UserEqptMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserEqptMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when User equipment configuration mismatch is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-997 UserPayloadMismatch

Alarm	Attributes	Applicable major release
Name: UserPayloadMismatch (4604) Type: communicationsAlarm Package: equipment.UserPayloadMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Upm	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when GFP User Payload Mismatch is detected.		
Remedial action: 1 Locate the OT with the UPM defect. Verify the encapsulation mode value.2 Locate the OT at the opposite end of the link. Ensure that the provisioning for the encapsulation mode parameter is the same for each OT.		

Table 3-998 UserPayloadMismatchOut

Alarm	Attributes	Applicable major release
Name: UserPayloadMismatchOut (5507) Type: communicationsAlarm Package: equipment.UserPayloadMismatchOut Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GfpUpm Applicable probable causes: • GfpUpm • GFPUPM	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Outgoing GFP User Payload Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-999 VcatLossOfAlignment

Alarm	Attributes	Applicable major release
Name: VcatLossOfAlignment (4605) Type: communicationsAlarm Package: equipment.VcatLossOfAlignment Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VcgLoa	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when VCG Loss of alignment is detected.		

Table 3-999 VcatLossOfAlignment (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that a loss of alignment has occurred in the virtual concatenation. Please follow the below steps to clear this alarm:\n 1. Verify the end-to-end path of the 11STMM10 circuit to ensure that the card reporting the alarm is connected to a 11STMM10 on the far end. A possible cause of this alarm is if the card is connected to another valid OC-48 signal generated by a test set or SONET interface, but which does not include two GFP encapsulated 1 GbE signals. Perform a warm card reset of the 11STMM10 reporting the alarm.\n 2. Perform a warm reset of the far end 11STMM10 that is connected to the 11STMM10 reporting the alarm.\n 3. Perform a cold reset of the far end 11STMM10 that is connected to the 11STMM10 reporting the alarm.\n 4. Reset the card of the far end 11STMM10 that is connected to the 11STMM10 reporting the alarm.\n 5. Replace the 11STMM10 reporting the alarm.\n For Detailed steps Please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 3-1000 VcgServerSignalFailure

Alarm	Attributes	Applicable major release
Name: VcgServerSignalFailure (4606) Type: communicationsAlarm Package: equipment.VcgServerSignalFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VcgSsf	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when VCG Server Signal Failure is detected.		
Remedial action: This alarm indicates that the OT has detected a VCG Server Signal Failure. This rare condition is raised when the time slots are incorrect.\n To clear this alarm, verify that the time slot information on the 11STMM10 line port and ODU1 are correctly provisioned on each end of the optical link. If not, use the following CLI commands to ensure timeslots are provisioned the same:\n Config interface 11STMM10 shelf slot/C{1-10} 1gbe timeslot line 1-4\n Config interface 11stmm10 shelf slot/C{1-10} 1gbe timeslot vts 0 or 1,4,7,10,13,16,19,22,25,28,31,34,37,40,43,46		

Table 3-1001 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 3-1002 VoltageHigh

Alarm	Attributes	Applicable major release
Name: VoltageHigh (3554) Type: equipmentAlarm Package: equipment.VoltageHigh Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VoltageHigh	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when High Input Voltage Defect is detected.		

Table 3-1002 VoltageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Using a DC voltmeter, measure the power going to the shelf and verify that it is within the accepted limits for proper operation (-48 to -52 volts). 2. Perform a warm reset on the Equipment Controller that is raising the PWR condition. 3. Perform a cold reset on the Equipment Controller that is raising the PWR condition. 4. Reseat the Equipment Controller that is raising the PWR condition. 5. Replace the Equipment Controller that is raising the PWR condition. Follow the return and repair process to return the card to an authorized repair center for replacement.		

Table 3-1003 VoltageLow

Alarm	Attributes	Applicable major release
Name: VoltageLow (3555) Type: equipmentAlarm Package: equipment.VoltageLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VoltageLow	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when VBatt magnitude below nominal range is detected.		
Remedial action: 1. Check the breakers for the alarmed shelf and verify that they are ON. 2. Using a DC voltmeter, measure the power going to the shelf and verify that it is within the accepted limits for proper operation (-48 to -52 volts). 3. Perform a warm reset on the Equipment Controller that is raising the PWR condition. 4. Perform a cold reset on the Equipment Controller that is raising the PWR condition. 5. Reseat the Equipment Controller that is raising the PWR condition. 6. Replace the Equipment Controller that is raising the PWR condition. Follow the return and repair process to return the card to an authorized repair center for replacement		

Table 3-1004 VtsForwardDefectIndication

Alarm	Attributes	Applicable major release
Name: VtsForwardDefectIndication (4607) Type: communicationsAlarm Package: equipment.VtsForwardDefectIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VTSFDI1	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when VTS Forward Defect Indication is detected.		
Remedial action: This alarm is raised when a problem has occurred upstream that causes an APS/PCC failure indication on the Virtual Time Slot[n] received by the 11DPE12/11DPE12E.\n Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Check the alarms/conditions along the OCh trail.\n 2. Identify the farthest upstream alarm/condition relative to the far end OTU2 port or client GBE port.\n 3. Check the OTU2 line port and client GBE port.\n 4. Follow the procedure for clearing identified alarm condition.		

Table 3-1005 VtsOpenConnectionIndication

Alarm	Attributes	Applicable major release
Name: VtsOpenConnectionIndication (4608) Type: communicationsAlarm Package: equipment.VtsOpenConnectionIndication Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VTSOCI1	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when VTS Open Connection Indication is detected.		

Table 3-1005 VtsOpenConnectionIndication (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the downstream 11DPE12/11DPE12E OT receives an APS/PCC message indicating an OCI from the upstream OT. This alarm is raised at the downstream OT on the Virtual Time Slot[n] which has an established connection.\n To clear this alarm, check the upstream 11DPE12/11DPE12E OT for any alarms/conditions on any VTS[n] with electrical connections. This will cause the OT to send an OCI message for the relevant VTS[n] to the downstream OT. An electrical connection is a provisioned connection from the VTS[n] to a GbE client port or another line VTS. If such an alarm is present, go to the procedure for clearing OCI alarms to clear the VTSOCI alarm at the downstream 11DPE12/11DPE12E OT.		

Table 3-1006 VwmIDFail

Alarm	Attributes	Applicable major release
Name: VwmIDFail (8462) Type: equipmentAlarm Package: equipment.VwmIDFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmIDFail	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: VWM shelf connected on PSS-EC card failed		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-1007 WaveKeyInsertionFailure

Alarm	Attributes	Applicable major release
Name: WaveKeyInsertionFailure (4609) Type: communicationsAlarm Package: equipment.WaveKeyInsertionFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Mod	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Card degrade - wavelength tracker channel id insertion is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 3-1008 WaveKeyOverlap

Alarm	Attributes	Applicable major release
Name: WaveKeyOverlap (2117) Type: communicationsAlarm Package: equipment.WaveKeyOverlap Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OchKeyOverlap	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Wave Key overlap is detected.		
Remedial action: 1. Perform the procedure Path Power Trace to identify the endpoints of the service for the particular alarmed channel.2. List the cross connects that currently exist on the endpoint NEs and identify the cross connects involved with the alarmed power trace. 3. Rekey the associated connections identified in Step 2.		

Table 3-1009 WavelengthTrackerEncodeDegrade

Alarm	Attributes	Applicable major release
Name: WavelengthTrackerEncodeDegrade (2121) Type: equipmentAlarm Package: equipment. WavelengthTrackerEncodeDegrade Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MtcesurvDgr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port Degrade - wavelength tracker encode degrade is detected.		
Remedial action: Please refer section MTCESURVDGR (Port degrade - wavelength tracker encode degrade) in 1830 Troubleshooting guide.		

Table 3-1010 WavelengthTrackerFailure

Alarm	Attributes	Applicable major release
Name: WavelengthTrackerFailure (4610) Type: equipmentAlarm Package: equipment.WavelengthTrackerFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Contr Applicable probable causes: • Contr • ContrOut	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Port degrade - wavelength tracker detection failure is detected.		
Remedial action: 1 Perform a warm reset of the card.2 Perform a cold reset of the card.3 Reseat the Card.4 Replace the Card. Action update pending.For Details Refer Procedure : Clear Port degrade - wavelength tracker communication failure in 1830 Troubleshooting guide.		

Table 3-1011 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 3-1012 WrongDevicePresent

Alarm	Attributes	Applicable major release
Name: WrongDevicePresent (4967) Type: equipmentAlarm Package: rmd.WrongDevicePresent Raised on class: rmd.Device	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdWDP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when there is an incorrect device found.		
Remedial action: Please ensure that the configure device type of the RMD is correct.		

Table 3-1013 WrongUnitInserted

Alarm	Attributes	Applicable major release
Name: WrongUnitInserted (4968) Type: equipmentAlarm Package: rmd.WrongUnitInserted Raised on class: rmd.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RmdIfWUP	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the wrong unit is inserted in a RMD device of type cEDD. Applicable to both customer and network ports.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action		

Table 3-1014 WtocmaOsnrOomr

Alarm	Attributes	Applicable major release
Name: WtocmaOsnrOomr (4611) Type: communicationsAlarm Package: equipment.WtocmaOsnrOomr Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WTOCMA_OSNROOMR	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Channel OSNR is out of valid measurement range is detected.		
Remedial action: The Channel OSNR is out of valid measurement range alarm is cleared automatically at the end of first complete interval during which the updated measuring OSNR value is in the valid measuring range (from 10dB to 25dB).		

Table 3-1015 WTR

Alarm	Attributes	Applicable major release
Name: WTR (3927) Type: equipmentAlarm Package: optical.WTR Raised on class: optical.LineReference	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Wtr	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: Switching applications - Set on working path of an SNCP when switching is revertive and effects have cleared on the working path and the Wait-to-Restore timer is in effect. \nPhotonic applications - The OT port has detected WTR at the LINEREF layer. A LINEREF detects WTR when on a timing reference and defects have cleared and the Wait to Restore timer is in effect. .		
Remedial action: Check the reference status.		

Table 3-1016 XcMismatch

Alarm	Attributes	Applicable major release
Name: XcMismatch (11133) Type: communicationsAlarm Package: equipment.XcMismatch Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: XcMismatch	Release: • 2.3 • 2.5 • 3.0 • 3.5 • 3.6 • 5.0 • 5.1 • 5.5 • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Cross Connection Mismatch .		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

4 1830 VWM OSU

4.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 4-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 8.2.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 4-2 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 8.2.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 4-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.2.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 4-4 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.2.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 4-5 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 8.2.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		

Table 4-5 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 4-6 BoardEqpt

Alarm	Attributes	Applicable major release
Name: BoardEqpt (3338) Type: equipmentAlarm Package: equipment.BoardEqpt Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BoardEqpt	Release: • 8.2.0
Description: The alarm is raised when Card failure - boot failure is detected.		
Remedial action: The alarm is raised when a card fails to initialize.See relevant section in 1830 Troubleshooting guide for detailed corrective action.		

Table 4-7 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 4-8 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		

Table 4-8 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 4-9 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 8.2.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 4-10 Breaker1BatteryFeedDown

Alarm	Attributes	Applicable major release
Name: Breaker1BatteryFeedDown (4446) Type: equipmentAlarm Package: equipment.Breaker1BatteryFeedDown Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Pwr	Release: • 8.2.0
Description: The alarm is raised when Power Filter 1 off or voltage low is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 4-11 CabinAlarm1

Alarm	Attributes	Applicable major release
Name: CabinAlarm1 (11192) Type: equipmentAlarm Package: vwm.CabinAlarm1 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CabinAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external cabin alarm input 1 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-12 CabinAlarm2

Alarm	Attributes	Applicable major release
Name: CabinAlarm2 (11193) Type: equipmentAlarm Package: vwm.CabinAlarm2 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CabinAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external cabin alarm input 2 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-13 CabinAlarm3

Alarm	Attributes	Applicable major release
Name: CabinAlarm3 (11194) Type: equipmentAlarm Package: vwm.CabinAlarm3 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CabinAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external cabin alarm input 3 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-14 CabinAlarm4

Alarm	Attributes	Applicable major release
Name: CabinAlarm4 (11195) Type: equipmentAlarm Package: vwm.CabinAlarm4 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CabinAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external cabin alarm input 4 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-15 CardInitializing

Alarm	Attributes	Applicable major release
Name: CardInitializing (1989) Type: equipmentAlarm Package: equipment.CardInitializing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardInit	Release: • 8.2.0
Description: The alarm is raised when Card initializing is detected.		
Remedial action: This condition should clear by itself, or be replaced by another card alarm. No corrective action is required.The condition clears or is replaced by a card alarm. If the alarm does not clear, then follow the procedure - Card Failure.Note: To get correct PM counts after an MSC cold reboot, initialize the PM registers.		

Table 4-16 CardMissing

Alarm	Attributes	Applicable major release
Name: CardMissing (1990) Type: equipmentAlarm Package: equipment.CardMissing Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplUnitMiss	Release: • 8.2.0
Description: The alarm is raised when Card missing is detected.		
Remedial action: The process for variable 1830 PSS nodes are different to clear this alarm.Please refer 1830 Trouble Shooting guide, section - REPLUNTMISS (Card Missing) to follow detailed steps for clearing this alarm.		

Table 4-17 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.2.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 4-18 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 8.2.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 4-19 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 4-20 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 4-21 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 4-22 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 8.2.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 4-23 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 8.2.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		

Table 4-23 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 4-24 EqptDgrOch

Alarm	Attributes	Applicable major release
Name: EqptDgrOch (3349) Type: communicationsAlarm Package: equipment.EqptDgrOch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgrOch	Release: • 8.2.0
Description: The alarm is raised when Port degrade - wavelength tracker communication failure is detected.		
Remedial action: This alarm is related to Port Degrade - Wavelength Tracker Communication Failure.1. Perform a warm reset of the card. 2. Perform a cold reset of the card. 3.Resett the card.4. Replace the card.		

Table 4-25 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 4-26 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		

Table 4-26 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 4-27 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 8.2.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 4-28 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 8.2.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 4-29 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 8.2.0

Table 4-29 EquipmentRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 4-30 FrameAlarm1

Alarm	Attributes	Applicable major release
Name: FrameAlarm1 (11196) Type: equipmentAlarm Package: vwm.FrameAlarm1 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 1 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-31 FrameAlarm10

Alarm	Attributes	Applicable major release
Name: FrameAlarm10 (11197) Type: equipmentAlarm Package: vwm.FrameAlarm10 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 10 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-32 FrameAlarm11

Alarm	Attributes	Applicable major release
Name: FrameAlarm11 (11198) Type: equipmentAlarm Package: vwm.FrameAlarm11 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 11 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-33 FrameAlarm12

Alarm	Attributes	Applicable major release
Name: FrameAlarm12 (11199) Type: equipmentAlarm Package: vwm.FrameAlarm12 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 12triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-34 FrameAlarm2

Alarm	Attributes	Applicable major release
Name: FrameAlarm2 (11200) Type: equipmentAlarm Package: vwm.FrameAlarm2 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 2 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-35 FrameAlarm3

Alarm	Attributes	Applicable major release
Name: FrameAlarm3 (11201) Type: equipmentAlarm Package: vwm.FrameAlarm3 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 3 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-36 FrameAlarm4

Alarm	Attributes	Applicable major release
Name: FrameAlarm4 (11202) Type: equipmentAlarm Package: vwm.FrameAlarm4 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 4 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-37 FrameAlarm5

Alarm	Attributes	Applicable major release
Name: FrameAlarm5 (11203) Type: equipmentAlarm Package: vwm.FrameAlarm5 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 5 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-38 FrameAlarm6

Alarm	Attributes	Applicable major release
Name: FrameAlarm6 (11204) Type: equipmentAlarm Package: vwm.FrameAlarm6 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 6 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-39 FrameAlarm7

Alarm	Attributes	Applicable major release
Name: FrameAlarm7 (11205) Type: equipmentAlarm Package: vwm.FrameAlarm7 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 7 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-40 FrameAlarm8

Alarm	Attributes	Applicable major release
Name: FrameAlarm8 (11206) Type: equipmentAlarm Package: vwm.FrameAlarm8 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 8 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-41 FrameAlarm9

Alarm	Attributes	Applicable major release
Name: FrameAlarm9 (11207) Type: equipmentAlarm Package: vwm.FrameAlarm9 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FrameAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external frame alarm 9 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-42 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.2.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 4-43 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.2.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 4-44 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.2.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 4-45 InterShelfLossofComms

Alarm	Attributes	Applicable major release
Name: InterShelfLossofComms (4495) Type: equipmentAlarm Package: equipment.InterShelfLossofComms Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ContCom	Release: • 8.2.0
Description: The alarm is raised when Inter-shelf loss of communication is detected.		
Remedial action: Refer Procedure : Clear Inter-shelf loss of communication alarm in 1830 Troubleshooting guide.		

Table 4-46 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 8.2.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 4-47 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 8.2.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 4-48 LineFacilityLoopbackActive

Alarm	Attributes	Applicable major release
Name: LineFacilityLoopbackActive (4502) Type: equipmentAlarm Package: equipment.LineFacilityLoopbackActive Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LpbkLine	Release: • 8.2.0
Description: The alarm is raised when Line Facility loopback active is detected.		
Remedial action: 1 Remove the loopback from the port.For CLI config interface <shelf slot port> loopback line disabled		

Table 4-49 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 8.2.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 4-50 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 8.2.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 4-51 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 4-52 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 8.2.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 4-52 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 4-53 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 8.2.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 4-54 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 8.2.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 4-55 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 8.2.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 4-56 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 4-57 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 8.2.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 4-58 OpticalPowerReceivedOutOfRange

Alarm	Attributes	Applicable major release
Name: OpticalPowerReceivedOutOfRange (2064) Type: communicationsAlarm Package: equipment. OpticalPowerReceivedOutOfRange Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OprOOR	Release: • 8.2.0
Description: The alarm is raised when Optical power received out of range is detected.		
Remedial action: This alarm indicates that the OT port has detected a received optical power out of range at OCH Layer. Please follow the below steps to clear this alarm:\n 1. Retrieve power level reading on the local port.\n 2. If input power level is lower or higher than required on the port, identify the associated OCh trail and verify the power levels along the OCh trail. If power levels along the upstream OCh trail are outside of their targeted range, then troubleshoot the port before continuing. If any power deviations raise additional alarms, troubleshoot them first.\n 3. If all power levels along the OCh trails fall within the target range, locate the fiber connected directly to receiver of the port.\n 4. Clean the fiber and check it for kinks.\n 5. If step 3 does not clear the alarm, replace the fiber.\n 6. Clean the input port of the OT. If the port is pluggable module, replace the module.		

Table 4-59 OpticsModuleMismatch

Alarm	Attributes	Applicable major release
Name: OpticsModuleMismatch (2065) Type: equipmentAlarm Package: equipment.OpticsModuleMismatch Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MismatchSfpXfp	Release: • 8.2.0
Description: The alarm is raised when Pluggable Module mismatch is detected.		
Remedial action: This alarm indicates that either the detected shelf identifier does not match the provisioned shelf identifier, or a pluggable module is installed on an Egress LD. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Verify the type of pluggable module that is currently installed into the alarmed card.\n 2. If the inserted pluggable module is of correct type by the service record but the MODULETYPE attribute is not correct, then modify the MODULETYPE value.\n 3. If the inserted pluggable module is of the incorrect type, then remove the module and insert one that matches the expected module type.\n 4. If the inserted pluggable module is of the correct type, then remove the module and reseat it back into the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 4-60 OpticsModuleUnknown

Alarm	Attributes	Applicable major release
Name: OpticsModuleUnknown (3386) Type: equipmentAlarm Package: equipment.OpticsModuleUnknown Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnknownSfpXfp	Release: • 8.2.0
Description: The alarm is raised when Pluggable Module unknown is detected.		

Table 4-60 OpticsModuleUnknown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that the optics module(pluggable module) inserted in the port is of type that is not recognized and the system cannot obtain manufacturing information of the unit. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. To clear the pack while it is still in service, do one of the following:\n a. Change the notification from a standing alarm to a transient condition, or\n b. Change the MODULETYPE provisioning(from "auto" to "user").\n 2. Perform a warm reset of the card.\n 3. Remove the pluggable module and examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage.\n 4. Remove and replace the pluggable module with another unit of the same type.\n 5. Perform a cold reset of the card.\n 6. Reseat the card.\n 7. If there is no transmission, check that the provisioned signal rate is supported by the pluggable module.\n 8. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 4-61 osuCardUnknown

Alarm	Attributes	Applicable major release
Name: osuCardUnknown (11134) Type: equipmentAlarm Package: equipment.osuCardUnknown Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Unknown	Release: • 8.2.0
Description: The alarm is raised when Card unknown is detected.		
Remedial action: 1. Verify if the inserted card is supported for the current running release.2. If the card is not yet supported in this release and the card is a required type for the NE, verify that the correct release is running on the NE. Upgrade the NE to the correct release if it is not to support this card type.3. If the NE is running the correct release but the card is not yet supported in that release, remove the card and replace it with one that is supported by the software running on the NE.4. If the card is supported and the NE is running the correct release, the problem may be with the card itself.5. Perform a warm reset of the card.6.Perform a cold reset of the card.7. Reset the card.8. Replace the card.		

Table 4-62 osuInMaintenance

Alarm	Attributes	Applicable major release
Name: osuInMaintenance (11135) Type: equipmentAlarm Package: equipment.osuInMaintenance Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Man	Release: • 8.2.0
Description: The alarm is raised when Manually caused abnormal condition - in maintenance is detected.		
Remedial action: Proceed as follows to clear the Manually caused abnormal condition - card in maintenance alarm.1 Manually place the card in service using the following command:CLI config slot shelf slot state up.		

Table 4-63 osuIntTempHigh

Alarm	Attributes	Applicable major release
Name: osuIntTempHigh (11136) Type: equipmentAlarm Package: equipment.osuIntTempHigh Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempHigh	Release: • 8.2.0
Description: The alarm is raised when over temperature is detected.		
Remedial action: Perform the steps in the procedure - High Temperature Troubleshooting.1. Verify that the fan tray is installed and that no fan tray alarms are present.Correct any faults found.2. Visually inspect the shelf to confirm that filler cards are installed in all empty slots in the shelf. This helps ensure proper airflow.3. Check for a dirty air filter. Clean or replace it as necessary. Contact your service representative for replacement filters.4. Use a thermometer to measure the ambient air temperature at the intake of the fans. Verify that the ambient temperature is not abnormally high. If the ambient temperature is too high, the NE may require additional cooling to bring it back to an acceptable operating temperature.5. Verify if other cards in the shelf report temperatures near their upper limit (within 10 degree Celsius).6. Replace the card and follow the return and repair process in the Customer and Product Support guide to return the faulty card to an authorized repair center for replacement.		

Table 4-64 osuSoftwareUpgradeFailure

Alarm	Attributes	Applicable major release
Name: osuSoftwareUpgradeFailure (11137) Type: equipmentAlarm Package: equipment.osuSoftwareUpgradeFailure Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwUpgFail	Release: • 8.2.0
Description: The alarm is raised when Software upgrade failed is detected.		
Remedial action: For 1830 VWM Node.Refer section SWUPGFAIL (Software Upgrade Failed) in 1830 VWM TroubleShooting guide.		

Table 4-65 osuSoftwareVersionMismatch

Alarm	Attributes	Applicable major release
Name: osuSoftwareVersionMismatch (11138) Type: communicationsAlarm Package: equipment.osuSoftwareVersionMismatch Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfMismatch Applicable probable causes: • SfMismatch • SWMISM	Release: • 8.2.0
Description: The alarm is raised when Software version mismatch is detected.		
Remedial action: This alarm is raised under the following conditions:\n a. The software on the alarmed card does not match the software on the nearest EC card because the card failed to update successfully.\n b. When all cards are not running the same software release. Please follow the below steps to clear this alarm(At the end of each step wait to see if the fault clears. If not proceed with the next step):\n 1. Find the software version number and release number on the EC card. Compare the corresponding number in the alarmed card. If it is not the same, download the software from EC to the alarmed card.\n 2. Contact your Nokia support representative.		

Table 4-66 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.2.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 4-67 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 8.2.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 4-68 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 8.2.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		

Table 4-68 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 4-69 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 8.2.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 4-70 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 4-71 PortFailure

Alarm	Attributes	Applicable major release
Name: PortFailure (2070) Type: equipmentAlarm Package: equipment.PortFailure Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FacTermDev Applicable probable causes: • FacTermDev • Eqpt • Mtcssurv	Release: • 8.2.0
Description: The alarm is raised when Pluggable Module SEEP failure is detected.		
Remedial action: This alarm indicates a port indicates a port initialization failure on the network ports(10G ports). Please follow the below steps to clear this alarm:\n 1. Perform a warm reset of the card.\n 2. Perform a cold reset of the card.\n 3. Reseat the card.\n 4. Remove the pluggable module from the port. Examine the connector on the pluggable module and the receptacle connector on the card where the pluggable module plugs into for any damage.\n 5. Remove and replace the pluggable module with another unit of the same type.\n 6. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 4-72 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 8.2.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 4-73 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 8.2.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		

Table 4-73 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 4-74 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 8.2.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 4-75 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 8.2.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 4-76 ReplUnitMissMOD

Alarm	Attributes	Applicable major release
Name: ReplUnitMissMOD (3392) Type: equipmentAlarm Package: equipment.ReplUnitMissMOD Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplUnitMissMOD	Release: • 8.2.0
Description: The alarm is raised when Pluggable Module missing is detected.		
Remedial action: This alarm indicates that the optics module(pluggable module) for the port is missing or the card is not able to successfully detect the presence of the module. Please follow the below steps to clear this alarm:\n 1. If there is no pluggable module in the port where the pluggable module missing condition is raised, then insert one that is appropriate for that transponder card.\n 2. Perform a warm reset of the card.\n 3. Remove the pluggable module from the port on the card it is inserted in. Examine the connector on the SFP and the receptacle connector on the card where the SFP plugs into for any damage. If no damage is seen, then reinsert the pluggable module into its port.\n 4. Remove and replace the pluggable module with another unit of the same type.\n 5. Perform a cold reset of the card.\n 6. Reseat the card.\n 7. Replace the card.\n For detailed steps please refer 1830 PSS Maintenance and Trouble-Clearing User Guide.		

Table 4-77 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 8.2.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 4-78 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 4-78 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 4-79 SfpTrmtPwrOOR

Alarm	Attributes	Applicable major release
Name: SfpTrmtPwrOOR (4552) Type: communicationsAlarm Package: equipment.SfpTrmtPwrOOR Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SfpTrmtPwrOOR	Release: • 8.2.0
Description: The alarm is raised when SFP or XFP optical transmit power out of range is detected.		
Remedial action: Please refer 1830 Troubleshooting guide for detailed steps for corrective action.		

Table 4-80 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 4-81 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.2.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		

Table 4-81 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 4-82 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.2.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 4-83 TCvPcs15Min

Alarm	Attributes	Applicable major release
Name: TCvPcs15Min (3416) Type: qualityOfServiceAlarm Package: equipment.TCvPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCS_15MIN	Release: • 8.2.0
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-84 TCvPcs1Day

Alarm	Attributes	Applicable major release
Name: TCvPcs1Day (3417) Type: qualityOfServiceAlarm Package: equipment.TCvPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_CV_PCS_1DAY	Release: • 8.2.0

Table 4-84 TCvPcs1Day (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Indicates a CV-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-85 TEsPcs15Min

Alarm	Attributes	Applicable major release
Name: TEsPcs15Min (3436) Type: qualityOfServiceAlarm Package: equipment.TEsPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCS_15MIN	Release: • 8.2.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-86 TEsPcs1Day

Alarm	Attributes	Applicable major release
Name: TEsPcs1Day (3437) Type: qualityOfServiceAlarm Package: equipment.TEsPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_ES_PCS_1DAY	Release: • 8.2.0
Description: The alarm is raised when Indicates a ES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-87 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 8.2.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		

Table 4-87 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 4-88 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 8.2.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 4-89 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 8.2.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 4-90 TSefsPcs15Min

Alarm	Attributes	Applicable major release
Name: TSefsPcs15Min (3498) Type: qualityOfServiceAlarm Package: equipment.TSefsPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCS_15MIN	Release: • 8.2.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-91 TSefsPcs1Day

Alarm	Attributes	Applicable major release
Name: TSefsPcs1Day (3499) Type: qualityOfServiceAlarm Package: equipment.TSefsPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SEFS_PCS_1DAY	Release: • 8.2.0
Description: The alarm is raised when Indicates a SEFS-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-92 TSesPcs15Min

Alarm	Attributes	Applicable major release
Name: TSesPcs15Min (3518) Type: qualityOfServiceAlarm Package: equipment.TSesPcs15Min Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCS_15MIN	Release: • 8.2.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-93 TSesPcs1Day

Alarm	Attributes	Applicable major release
Name: TSesPcs1Day (3519) Type: qualityOfServiceAlarm Package: equipment.TSesPcs1Day Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: T_SES_PCS_1DAY	Release: • 8.2.0
Description: The alarm is raised when Indicates a SES-PCS Threshold Crossing detection is detected.		
Remedial action: The alarm is raised when the related TCA threshold is crossed.Check min/max range of valid values for this TCA in order to clear the alarm.		

Table 4-94 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 8.2.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 4-95 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 8.2.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 4-96 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 8.2.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 4-97 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 8.2.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 4-98 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 8.2.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 4-99 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 8.2.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 4-100 UserAlarm1

Alarm	Attributes	Applicable major release
Name: UserAlarm1 (11208) Type: equipmentAlarm Package: vwm.UserAlarm1 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 1 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-101 UserAlarm10

Alarm	Attributes	Applicable major release
Name: UserAlarm10 (11209) Type: equipmentAlarm Package: vwm.UserAlarm10 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 10 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-102 UserAlarm11

Alarm	Attributes	Applicable major release
Name: UserAlarm11 (11210) Type: equipmentAlarm Package: vwm.UserAlarm11 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 11 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-103 UserAlarm12

Alarm	Attributes	Applicable major release
Name: UserAlarm12 (11211) Type: equipmentAlarm Package: vwm.UserAlarm12 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 12 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-104 UserAlarm13

Alarm	Attributes	Applicable major release
Name: UserAlarm13 (11212) Type: equipmentAlarm Package: vwm.UserAlarm13 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 13 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-105 UserAlarm14

Alarm	Attributes	Applicable major release
Name: UserAlarm14 (11213) Type: equipmentAlarm Package: vwm.UserAlarm14 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 14 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-106 UserAlarm15

Alarm	Attributes	Applicable major release
Name: UserAlarm15 (11214) Type: equipmentAlarm Package: vwm.UserAlarm15 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 15 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-107 UserAlarm16

Alarm	Attributes	Applicable major release
Name: UserAlarm16 (11215) Type: equipmentAlarm Package: vwm.UserAlarm16 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 16 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-108 UserAlarm17

Alarm	Attributes	Applicable major release
Name: UserAlarm17 (11216) Type: equipmentAlarm Package: vwm.UserAlarm17 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 17 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-109 UserAlarm18

Alarm	Attributes	Applicable major release
Name: UserAlarm18 (11217) Type: equipmentAlarm Package: vwm.UserAlarm18 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 18 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-110 UserAlarm19

Alarm	Attributes	Applicable major release
Name: UserAlarm19 (11218) Type: equipmentAlarm Package: vwm.UserAlarm19 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 19 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-111 UserAlarm2

Alarm	Attributes	Applicable major release
Name: UserAlarm2 (11219) Type: equipmentAlarm Package: vwm.UserAlarm2 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 2 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-112 UserAlarm20

Alarm	Attributes	Applicable major release
Name: UserAlarm20 (11220) Type: equipmentAlarm Package: vwm.UserAlarm20 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 20 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-113 UserAlarm21

Alarm	Attributes	Applicable major release
Name: UserAlarm21 (11221) Type: equipmentAlarm Package: vwm.UserAlarm21 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 21 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-114 UserAlarm22

Alarm	Attributes	Applicable major release
Name: UserAlarm22 (11222) Type: equipmentAlarm Package: vwm.UserAlarm22 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 22 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-115 UserAlarm23

Alarm	Attributes	Applicable major release
Name: UserAlarm23 (11223) Type: equipmentAlarm Package: vwm.UserAlarm23 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 23 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-116 UserAlarm24

Alarm	Attributes	Applicable major release
Name: UserAlarm24 (11224) Type: equipmentAlarm Package: vwm.UserAlarm24 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 24 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-117 UserAlarm25

Alarm	Attributes	Applicable major release
Name: UserAlarm25 (11225) Type: equipmentAlarm Package: vwm.UserAlarm25 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 25 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-118 UserAlarm26

Alarm	Attributes	Applicable major release
Name: UserAlarm26 (11226) Type: equipmentAlarm Package: vwm.UserAlarm26 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 26 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-119 UserAlarm27

Alarm	Attributes	Applicable major release
Name: UserAlarm27 (11227) Type: equipmentAlarm Package: vwm.UserAlarm27 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 27 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-120 UserAlarm28

Alarm	Attributes	Applicable major release
Name: UserAlarm28 (11228) Type: equipmentAlarm Package: vwm.UserAlarm28 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 28 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-121 UserAlarm29

Alarm	Attributes	Applicable major release
Name: UserAlarm29 (11229) Type: equipmentAlarm Package: vwm.UserAlarm29 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 29 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-122 UserAlarm3

Alarm	Attributes	Applicable major release
Name: UserAlarm3 (11230) Type: equipmentAlarm Package: vwm.UserAlarm3 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 3 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-123 UserAlarm30

Alarm	Attributes	Applicable major release
Name: UserAlarm30 (11231) Type: equipmentAlarm Package: vwm.UserAlarm30 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 30 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-124 UserAlarm31

Alarm	Attributes	Applicable major release
Name: UserAlarm31 (11232) Type: equipmentAlarm Package: vwm.UserAlarm31 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 31 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-125 UserAlarm32

Alarm	Attributes	Applicable major release
Name: UserAlarm32 (11233) Type: equipmentAlarm Package: vwm.UserAlarm32 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 32 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-126 UserAlarm4

Alarm	Attributes	Applicable major release
Name: UserAlarm4 (11234) Type: equipmentAlarm Package: vwm.UserAlarm4 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 4 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-127 UserAlarm5

Alarm	Attributes	Applicable major release
Name: UserAlarm5 (11235) Type: equipmentAlarm Package: vwm.UserAlarm5 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 5 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-128 UserAlarm6

Alarm	Attributes	Applicable major release
Name: UserAlarm6 (11236) Type: equipmentAlarm Package: vwm.UserAlarm6 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 6 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-129 UserAlarm7

Alarm	Attributes	Applicable major release
Name: UserAlarm7 (11237) Type: equipmentAlarm Package: vwm.UserAlarm7 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: U Raised by an SMM unit in case an external user alarm input 7 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-130 UserAlarm8

Alarm	Attributes	Applicable major release
Name: UserAlarm8 (11238) Type: equipmentAlarm Package: vwm.UserAlarm8 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 8 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-131 UserAlarm9

Alarm	Attributes	Applicable major release
Name: UserAlarm9 (11239) Type: equipmentAlarm Package: vwm.UserAlarm9 Raised on class: vwm.ExternalAlarmInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserAlarm	Release: • 8.2.0
Description: Raised by an SMM unit in case an external user alarm input 9 triggers		
Remedial action: Please check and correct the environmental condition indicated in the alarm at the remote site.		

Table 4-132 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 8.2.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		

Table 4-132 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 4-133 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 8.2.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

5 7210 SAS-D

5.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 5-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 5-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 5-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 5-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 5-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 5-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 5-7 AtcaFanFailure

Alarm	Attributes	Applicable major release
Name: AtcaFanFailure (1124) Type: equipmentAlarm Package: equipment.AtcaFanFailure Raised on class: equipment.Fan	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled') OR ('operationalState' EQUAL 'Down'))		
Clearing condition: (('operationalState' EQUAL 'Enabled') OR ('operationalState' EQUAL 'Up'))		
Remedial action: This alarm is raised if the fan speed falls below 500 rpm. If the alarm persists, replace the appropriate (upper or lower) fan tray.		

Table 5-8 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 5-9 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 5-10 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 5-11 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-11 BITS2ReferenceLossOfSignal (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 5-12 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 5-13 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 5-14 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 5-15 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 5-16 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-16 BITSReferenceOutOfFrequency (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 5-17 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 5-18 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 5-18 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 5-19 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 5-20 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		

Table 5-20 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 5-21 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 5-22 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 5-23 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 5-24 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 5-25 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 5-26 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 5-27 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 5-28 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 5-29 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 5-30 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 5-31 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-31 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 5-32 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-33 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		

Table 5-33 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 5-34 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 5-35 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 5-36 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 5-37 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 7.0.0 • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 5-38 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-38 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 5-39 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 5-40 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		

Table 5-40 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 5-41 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 5-42 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 5-43 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 5-44 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 5-45 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 5-46 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 5-47 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-47 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 5-48 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 5-49 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 5-49 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 5-50 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 5-51 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 5-52 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 5-53 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 5-54 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 5-55 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 5-56 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 5-57 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 5-58 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 5-59 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 5-60 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-60 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 5-61 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 5-62 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		

Table 5-62 MvrConfiguredFromVplsNotExist (continued)

Alarm	Attributes	Applicable major release
Remedial action: Create the missing MVR VPLS.		

Table 5-63 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNotExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 5-64 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 5-65 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 5-66 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 5-67 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 5-68 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 5-69 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 5-70 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 5-71 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		

Table 5-71 nonDeployedAdjacencyExists (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 5-72 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 5-73 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 5-74 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 5-75 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 5-76 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 5-77 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 5-78 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 5-79 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 5-80 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-81 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-82 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-82 PowerSupplyFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-83 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-84 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		

Table 5-84 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 5-85 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-86 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-87 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 5-88 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 5-89 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 5-90 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 5-91 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 5-92 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 5-93 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 5-94 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 5-95 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 5-96 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 5-97 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-97 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 5-98 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 5-99 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		

Table 5-99 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 5-100 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 5-101 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 5-102 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 5-103 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 5-104 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 5-105 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 5-106 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 5-107 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 5-108 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-108 StpRootGuardViolation (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 5-109 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 5-110 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		

Table 5-110 SubSysChassMemoryUsageHi (continued)

Alarm	Attributes	Applicable major release
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 5-111 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 5-112 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 5-113 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 5-114 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 5-115 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-115 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 5-116 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		

Table 5-116 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 5-117 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 5-118 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 5-119 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 5-120 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 5-121 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 5-122 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 5-123 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 5-123 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 5-124 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 5-125 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

6 7210 SAS-E

6.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 6-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 6-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 6-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 6-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 6-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 6-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 6-7 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 6-8 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 6-9 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 6-10 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 6-11 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 6-12 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 6-13 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 6-14 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 6-15 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-15 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 6-16 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 6-17 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 6-17 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 6-18 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 6-19 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 6-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 6-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 6-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-22 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 6-23 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-24 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		

Table 6-24 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 6-25 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 6-26 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 6-27 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 6-28 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 6-29 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 6-30 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 6-31 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 6-32 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 6-33 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 6-34 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 6-35 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 6-36 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 6-37 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 6-38 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 6-39 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 6-40 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 6-41 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 6-42 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 6-43 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 6-44 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 6-45 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 6-46 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 6-47 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 6-48 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 6-49 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-49 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 6-50 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 6-51 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		

Table 6-51 MvrConfiguredFromVplsNotExist (continued)

Alarm	Attributes	Applicable major release
Remedial action: Create the missing MVR VPLS.		

Table 6-52 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 6-53 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 6-54 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 6-55 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 6-56 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 6-57 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 6-58 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 6-59 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 6-60 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		

Table 6-60 nonDeployedAdjacencyExists (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 6-61 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 6-62 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 6-63 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 6-64 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 6-65 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 6-66 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 6-67 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 6-68 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 6-69 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-70 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-71 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-71 PowerSupplyFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-72 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-73 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		

Table 6-73 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 6-74 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-75 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-76 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 6-77 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 6-78 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 6-79 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 6-80 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 6-81 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 6-82 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 6-83 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 6-84 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 6-85 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 6-86 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 6-87 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override'))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 6-88 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 6-89 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 6-90 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 6-91 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 6-92 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-92 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 6-93 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 6-94 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 6-95 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 6-96 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 6-97 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 6-98 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 6-98 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 6-99 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 6-100 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 6-101 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 6-102 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 6-103 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 6-104 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 6-105 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 6-106 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 6-106 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 6-107 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 6-108 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		

Table 6-108 WrongCpaaSoftwareVersion (continued)

Alarm	Attributes	Applicable major release
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 6-109 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

7 7210 SAS-K

7.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 7-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 7-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 7-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 7-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 7-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 7-5 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 7-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override'))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 7-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 7-8 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 7-9 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 7-10 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		

Table 7-10 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 7-11 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 7-12 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 7-13 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 7-13 BITS2ReferenceOutOfFrequency (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 7-14 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 7-15 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 7-16 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 7-17 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 7-18 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 7-19 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 7-20 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 7-21 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 7-21 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 7-22 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 7-23 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 7-24 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 7-25 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 7-26 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 7-26 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 7-27 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 7-28 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 7-29 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 7-30 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 7-31 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		

Table 7-31 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 7-32 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 7-33 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-34 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 7-35 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 7-36 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 7-37 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 7-38 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 7-39 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		

Table 7-39 EthernetPortNoAmLock (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 7-40 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 7-41 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 7-42 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 7-43 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 7-44 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		

Table 7-44 ExternalTimingReferenceNotQualified (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 7-45 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 7-46 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 7-47 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 7-48 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 7-49 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		

Table 7-49 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 7-50 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 7-51 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 7-52 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 7-53 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 7-54 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 7-55 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 7-56 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 7-57 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 7-57 LagDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 7-58 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 7-59 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 7-60 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 7-61 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 7-62 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 7-63 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 7-64 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 7-65 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 7-66 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 7-67 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 7-68 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 7-69 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 9.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 7-70 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 7-71 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 7-71 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 7-72 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 7-73 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 7-74 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 7-75 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNotExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 7-76 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNotExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		

Table 7-76 MvrConfiguredProxySapNotExist (continued)

Alarm	Attributes	Applicable major release
Remedial action: Create the missing proxy SAP.		

Table 7-77 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 7-78 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 7-79 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 7-80 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 7-81 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 7-82 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 7-83 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 7-84 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 7-85 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 7-86 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 7-87 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 7-88 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 7-89 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		

Table 7-89 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 7-90 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 7-91 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 7-92 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 7-93 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 7-94 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 7-94 PortEtherSymMonSDAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 7-95 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 7-96 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-97 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-98 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-99 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		

Table 7-99 PowerSupplyInputFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-100 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 7-101 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-102 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-103 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 7-104 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 7-105 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 7-106 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 7-107 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 7-108 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 7-109 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 7-110 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		

Table 7-110 PTPReferenceLossOfSignal (sonet) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 7-111 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 7-112 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 7-113 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 7-113 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 7-114 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 7-115 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 7-116 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 7-117 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 7-118 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 7-118 RsvpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 7-119 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 7-120 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 7-121 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 7-122 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 7-123 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		

Table 7-123 SdpEgressIfsNetDomainInConsistent (continued)

Alarm	Attributes	Applicable major release
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 7-124 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 7-125 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 7-126 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 7-127 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 9.0.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 7-128 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 7-129 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 7-130 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 7-131 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 7-131 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 7-132 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 7-133 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 7-134 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		

Table 7-134 TemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 7-135 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 7-136 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 7-137 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 7-138 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 7-138 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 7-139 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 7-140 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 7-141 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 7-142 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 7-143 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 7-144 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 7-145 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 7-146 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 7-147 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 7-148 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 7-149 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 7-150 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 7-151 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 7-152 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		

Table 7-152 WrongCpaaSoftwareVersion (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 7-153 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

8 7210 SAS-M

8.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 8-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 8-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 8-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 8-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 8-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 8-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 8-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 8-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 8-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 8-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 8-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 8-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 8-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-13 BfdInterfaceConnectionDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 8-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 8-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 8-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 8-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-18 BITS2ReferenceOutOfFrequency (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 8-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 8-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 8-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 8-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 8-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-23 BITSReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 8-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 8-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 8-25 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 8-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 8-27 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		

Table 8-27 CesBfrOverrun (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-28 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-29 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-30 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-31 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-32 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-33 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-34 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 8-35 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 8-36 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 8-37 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 8-38 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-38 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 8-39 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 8-40 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 8-41 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 8-42 DaughterCardConfigMissing

Alarm	Attributes	Applicable major release
Name: DaughterCardConfigMissing (4403) Type: equipmentAlarm Package: equipment.DaughterCardConfigMissing Raised on class: equipment.DaughterCardSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DaughterCardConfigMissing	Release: • 5.0.0
Description: The alarm is raised when a supported MDA is inserted into a slot, but the current configuration is not sufficient for the MDA to operate.		
Remedial action: A configuration error has occurred which must be corrected. The BOF configuration must be changed to include no-service-ports.		

Table 8-43 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-43 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 8-44 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 8-45 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 8-46 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 8-47 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 8-48 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-48 DS1E1ResourceAvailabilityIndicator (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 8-49 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 8-50 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 8-51 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 8-52 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 8-53 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 8-54 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 8-55 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-55 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-56 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 8-57 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		

Table 8-57 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 8-58 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 8-59 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 8-60 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 7.0.0 • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 8-61 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 8-62 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-62 EthernetPortHighBer (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 8-63 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 8-64 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		

Table 8-64 EthernetPortNoAmLock (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 8-65 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 8-66 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 8-67 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 8-68 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 8-69 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 8-70 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 8-71 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-71 FanTrayRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 8-72 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 8-73 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		

Table 8-73 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 8-74 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 8-75 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 8-76 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 8-77 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 8-78 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		

Table 8-78 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 8-79 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 8-80 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 8-81 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 8-82 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 8-83 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-83 inSufficientBandwidth (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 8-84 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 8-85 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 8-85 InterfaceDown (vpls) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 8-86 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 8-87 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 8-88 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 8-89 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 8-90 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-90 KeepAliveProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 8-91 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 8-92 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		

Table 8-92 LagDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 8-93 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 8-94 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 8-95 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 8-96 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 8-97 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-97 LicensedLimitExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 8-98 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 8-99 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 8-99 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 8-100 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 8-101 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 8-102 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 8-103 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 8-104 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-104 macMoveRateExceeded (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 8-105 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 8-106 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 8-106 MCLagDown (lag) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 8-107 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 8-108 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 8-109 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 8-110 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 8-111 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 8-112 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 8-113 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		

Table 8-113 MvrConfiguredProxySapNotExist (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 8-114 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 8-115 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 8-116 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 8-117 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 8-118 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 8-119 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 8-120 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 8-121 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 8-122 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		

Table 8-122 nonDeployedAdjacencyExists (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 8-123 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 8-124 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 8-125 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 8-126 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 8-127 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 8-128 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 8-129 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-130 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-131 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 8-132 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 8-133 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 8-134 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 8-135 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-135 PortEtherSymMonSDAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 8-136 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 8-137 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		

Table 8-137 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-138 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-139 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-140 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-141 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 8-142 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-143 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-144 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 8-145 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 8-146 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 8-147 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 8-148 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 8-149 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 8-150 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 8-151 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 8-152 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-152 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 8-153 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 8-154 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 8-154 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 8-155 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 8-156 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 8-157 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 8-158 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 8-159 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 8-160 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 8-161 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-161 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 8-162 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 8-163 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		

Table 8-163 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 8-164 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 8-165 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override'))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 8-166 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 8-167 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 8-168 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 8-169 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 8-170 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-170 StpExceptionCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 8-171 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 8-172 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 8-172 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 8-173 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 8-174 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 8-175 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 8-176 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 8-177 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 8-178 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 8-178 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.

Table 8-179 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 8-180 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 8-181 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 8-182 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-182 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 8-183 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 8-184 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 8-185 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 8-186 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 8-187 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 8-187 upgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 8-188 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 8-189 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 8-190 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 8-191 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 8-192 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 8-193 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 8-194 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 8-195 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

9 7210 SAS-Mxp

9.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 9-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 9-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 8.0.0 • 9.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 9-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 9-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 9-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 9-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 9-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 9-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		

Table 9-8 AsymmetricalConfig (multichassis) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 9-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 9-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 9-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 9-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 9-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 9-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 9-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 9-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 9-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 9-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 9-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 9-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 9-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 9-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 9-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 9-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 9-25 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 9-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 9-27 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 9-28 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 9-29 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 9-30 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 9-31 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 9-32 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 9-33 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 9-33 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 9-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 9-35 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 9-36 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 8.0.0 • 9.0.0

Table 9-36 DS1E1Looped (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 9-37 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 9-38 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 9-39 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 9-40 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 9-41 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		

Table 9-41 DS1E1SignalFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 9-42 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 9-43 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 9-44 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 9-45 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 9-46 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		

Table 9-46 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-47 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 9-48 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 9-49 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 9-50 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 9-51 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		

Table 9-51 EthernetPortCrcFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 9-52 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 9-53 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 9-54 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 9-55 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 9-56 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		

Table 9-56 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 9-57 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 9-58 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 9-59 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 9-60 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 9-61 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 9-62 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 9-63 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 9-64 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		

Table 9-64 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 9-65 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 9-66 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 9-67 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0

Table 9-67 GroupDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 9-68 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 9-69 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 9-70 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 9-71 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 9-72 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		

Table 9-72 IncorrectPeerSynchronizationPortConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 9-73 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 9-74 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 9-75 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		

Table 9-75 inSufficientBandwidth (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 9-76 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 9-77 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 9-78 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 9-79 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 9-80 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 9-81 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 9-82 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 9-83 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		

Table 9-83 LagPortAddFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 9-84 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 9-85 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 9-86 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		

Table 9-86 LdpTargetedPeerDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 9-87 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 9-88 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 9-89 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 9-90 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 9-91 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 9-92 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 9-93 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 9-94 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 9-95 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 9-96 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 9-97 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		

Table 9-97 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 9-98 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 9-99 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 9-100 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 9-101 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 9-102 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 9-103 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 9-104 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		

Table 9-104 MvrSiteDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 9-105 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-106 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 9-107 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 9-108 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 9-109 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 9-110 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 9-111 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 9-112 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 9-113 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-114 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 9-115 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		

Table 9-115 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 9-116 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 9-117 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 9-118 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0

Table 9-118 PeerDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-119 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-120 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 9-121 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 9-122 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 9-123 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		

Table 9-123 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 9-124 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 9-125 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 9-126 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-127 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-128 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-129 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-130 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 9-131 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-132 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-133 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 9-134 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 9-135 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 9-136 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 9-137 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 9-138 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 9-139 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 9-140 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 9-141 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPol-lInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 9-142 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 9-143 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 9-143 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 9-144 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam.RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 9-145 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 9-146 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 9-147 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 9-148 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 9-148 RipInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-149 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 9-150 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 9-151 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 9-152 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 9-153 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		

Table 9-153 SdpBindingDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 9-154 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 9-155 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 9-156 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 9-157 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 9-158 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		

Table 9-158 SessionDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 9-159 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-160 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 9-161 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		

Table 9-161 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 9-162 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 9-163 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 9-164 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 9-165 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 9-166 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 9-167 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 9-168 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 9-169 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		

Table 9-169 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 9-170 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 9-171 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 9-172 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 9-173 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		

Table 9-173 TunnelAdministrativelyDown (svt) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 9-174 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 9-175 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 9-176 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		

Table 9-176 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 9-177 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 9-178 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 9-179 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 9-180 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 9-181 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 9-182 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 9-183 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-184 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		

Table 9-184 VirtualNeighborDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 9-185 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 9-186 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 9-187 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

10 7210 SAS-R

10.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 10-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 10-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 10-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 10-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 10-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 10-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 10-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 10-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-7 AreaTypeMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 10-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 10-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 10-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 10-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 10-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		

Table 10-12 BfdInterfaceConnectionBroken (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 10-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 10-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 10-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 10-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		

Table 10-17 BITS2ReferenceLossOfSignal (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 10-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 10-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 10-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 10-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 10-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		

Table 10-22 BITSReferenceOutOfFrequency (sonet) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 10-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 10-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 10-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 10-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 10-27 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 10-28 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 10-29 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		

Table 10-29 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 10-30 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 10-31 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 10-32 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 10-33 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 10-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-34 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 10-35 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 10-36 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 10-37 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 10-38 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 10-39 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-39 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-40 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 10-41 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		

Table 10-41 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 10-42 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 10-43 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 10-44 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 7.0.0 • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 10-45 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 10-46 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		

Table 10-46 EthernetPortHighBer (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 10-47 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 10-48 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 10-49 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 10-50 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 10-51 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-51 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 10-52 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 10-53 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 10-54 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 10-55 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 10-56 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		

Table 10-56 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 10-57 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 10-58 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 10-59 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 10-60 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 10-61 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		

Table 10-61 IncompleteConfig (multichassis) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 10-62 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 10-63 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 10-64 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 10-65 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis. PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 10-66 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 10-66 InstanceDown (vrrp) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 10-67 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 10-68 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 10-69 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 10-70 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 10-71 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		

Table 10-71 IsisInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 10-72 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 10-73 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 10-74 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 10-75 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 10-76 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-76 LdpDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 10-77 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 10-78 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 10-79 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 10-80 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 10-81 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		

Table 10-81 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 10-82 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 10-83 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 10-84 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 10-85 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 10-86 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		

Table 10-86 macMoveRateExceeded (service) (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 10-87 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 10-88 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 10-89 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 10-90 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 10-91 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-91 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 10-92 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 10-93 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		

Table 10-93 MplsPathUpdateFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 10-94 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 10-95 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 10-96 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 10-97 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 10-98 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		

Table 10-98 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 10-99 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 10-100 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		

Table 10-100 NewSsh2ServerKeyDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 10-101 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 10-102 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 10-103 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 10-104 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 10-105 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		

Table 10-105 NTPOperDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 10-106 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 10-107 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 10-108 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 10-109 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 10-110 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-110 PeerConnectionDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 10-111 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-112 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-113 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 10-114 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 10-115 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 10-115 PimDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 10-116 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 10-117 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 10-118 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 10-119 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-120 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		

Table 10-120 PowerSupplyDcFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-121 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-122 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-123 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 10-124 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-125 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		

Table 10-125 PowerSupplyOverTemperature (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-126 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 10-127 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 10-128 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 10-129 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 10-130 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		

Table 10-130 PTPPeerLossOfAnnounce (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 10-131 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 10-132 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 10-133 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 10-134 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 10-135 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		

Table 10-135 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 10-136 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 10-137 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 10-138 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 10-139 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 10-140 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		

Table 10-140 RouteDistinguisherNotConfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 10-141 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 10-142 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 10-143 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 10-144 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 10-145 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-145 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 10-146 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 10-147 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		

Table 10-147 SecondaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 10-148 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 10-149 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 10-150 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 10-151 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 10-152 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 10-152 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 10-153 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 10-154 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 10-155 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 10-156 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 10-157 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-157 svcMacFdbTabelFull (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 10-158 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 10-159 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 10-160 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 10-161 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 10-162 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 10-163 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 10-163 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 10-164 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 10-165 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 10-166 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 10-167 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		

Table 10-167 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the network resources along the path.		

Table 10-168 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 10-169 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 10-170 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 10-171 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 10-172 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		

Table 10-172 upgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 10-173 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 10-174 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 10-175 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 10-176 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 10-177 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 10-177 VirtualNeighborDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 10-178 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 10-179 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 10-180 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

11 7210 SAS-Sx

11.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 11-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 11-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 8.0.0 • 9.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 11-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 11-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 11-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 11-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 11-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 11-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		

Table 11-8 AsymmetricalConfig (multichassis) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 11-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 11-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 11-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 11-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 11-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 11-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 11-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 11-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 11-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 11-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 11-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 11-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 11-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 11-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 11-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 11-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 11-25 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 11-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 11-27 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 11-28 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 11-29 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 11-30 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 11-31 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 11-32 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 11-33 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 11-33 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 11-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 11-35 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 11-36 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 8.0.0 • 9.0.0

Table 11-36 DS1E1Looped (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 11-37 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 11-38 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 11-39 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 11-40 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 11-41 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		

Table 11-41 DS1E1SignalFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 11-42 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 11-43 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 11-44 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 11-45 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 11-46 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		

Table 11-46 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-47 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 11-48 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 11-49 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 11-50 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 11-51 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		

Table 11-51 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 11-52 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 11-53 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 11-54 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 11-55 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 11-56 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 8.0.0 • 9.0.0

Table 11-56 EthernetPortNoFrameLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 11-57 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 11-58 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 11-59 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 11-60 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 11-61 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 11-62 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 11-63 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 11-64 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		

Table 11-64 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 11-65 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 11-66 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 11-67 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 11-68 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 11-69 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		

Table 11-69 IncorrectPeerConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 11-70 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 11-71 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis. PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 11-72 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 11-73 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 11-74 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 11-75 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 11-76 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 11-77 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 11-78 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 11-79 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 11-80 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 11-80 LagDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 11-81 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 11-82 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 11-83 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 11-84 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 11-85 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 11-86 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 11-87 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 11-88 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 11-89 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 11-90 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 11-91 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 11-92 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 11-93 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 11-94 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 11-94 MCLagDown (lag) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 11-95 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 11-96 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 11-97 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 11-98 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 11-99 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		

Table 11-99 MsPwFecRetryExpired (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 11-100 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNotExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 11-101 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNotExist	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 11-102 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 11-103 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 11-104 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 11-104 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 11-105 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 11-106 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 11-107 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 11-108 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 11-109 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 11-110 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 11-111 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 11-112 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		

Table 11-112 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 11-113 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 11-114 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 11-115 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 11-116 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-117 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-118 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 11-119 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 11-120 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 9.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 11-120 PimDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 11-121 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 11-122 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 11-123 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 11-124 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-125 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-126 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-127 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-128 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 11-129 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-130 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-131 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 11-132 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 11-133 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 11-134 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 11-135 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 11-136 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 11-137 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 11-138 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 11-139 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 11-140 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 8.0.0 • 9.0.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 11-141 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 11-142 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 11-143 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		

Table 11-143 RemoteMepCCMAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 11-144 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 11-145 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 11-146 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		

Table 11-146 SaveConfigFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 11-147 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 11-148 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 11-149 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 11-150 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 11-151 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		

Table 11-151 SecondaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 11-152 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 11-153 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 11-154 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 11-155 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 11-156 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 11-157 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 11-158 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 11-159 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 11-160 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 11-161 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 11-162 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 11-163 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 11-164 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 11-165 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		

Table 11-165 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 11-166 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 11-167 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 11-168 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 11-169 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 11-170 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 11-171 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 11-172 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 11-173 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 11-174 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 11-175 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 11-176 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 11-177 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 11-178 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 11-179 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 11-180 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 11-181 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		

Table 11-181 XplError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

12 7210 SAS-T

12.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 12-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 12-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 12-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 12-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 12-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 12-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 12-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 12-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-7 AreaTypeMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 12-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 12-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 12-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 12-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 12-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		

Table 12-12 BfdInterfaceConnectionBroken (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 12-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 12-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 12-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 12-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		

Table 12-17 BITS2ReferenceLossOfSignal (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 12-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 12-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 12-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 12-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 12-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		

Table 12-22 BITSReferenceOutOfFrequency (sonet) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 12-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 12-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 12-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 12-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 12-27 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 12-28 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 12-29 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		

Table 12-29 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 12-30 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 12-31 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 12-32 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 12-33 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 12-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-34 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 12-35 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 12-36 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 12-37 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 12-38 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 12-39 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		

Table 12-39 DS1E1ResourceAvailabilityIndicator (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 12-40 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 12-41 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 12-42 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 12-43 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 12-44 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-44 EquipmentDegraded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 12-45 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 12-46 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		

Table 12-46 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-47 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 12-48 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 12-49 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 12-50 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 12-51 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 7.0.0 • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		

Table 12-51 EthernetPortCrcFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 12-52 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 12-53 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 12-54 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 12-55 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 12-56 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-56 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 12-57 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 12-58 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		

Table 12-58 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 12-59 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 12-60 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 12-61 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 12-62 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 12-63 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		

Table 12-63 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 12-64 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 12-65 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 12-66 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 12-67 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 12-68 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		

Table 12-68 IncompleteConfig (multichassis) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 12-69 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 12-70 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 12-71 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortConfig Raised on class: multichassis.PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 12-72 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 12-73 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 12-73 InstanceDown (vrrp) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 12-74 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 12-75 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 12-76 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 12-77 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 12-78 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		

Table 12-78 IsisDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 12-79 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 12-80 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 12-81 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 12-82 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 12-83 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 12-84 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 12-85 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		

Table 12-85 LdpSessionNonexistent (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 12-86 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 12-87 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 12-88 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 12-89 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 12-90 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		

Table 12-90 LspDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 12-91 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 12-92 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 12-93 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 12-94 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 12-95 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		

Table 12-95 macMoveRateExceeded (svt) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 12-96 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 12-97 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 12-98 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 12-99 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 12-100 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		

Table 12-100 MplsDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 12-101 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 12-102 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 12-103 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNotExist	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 12-104 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNotExist	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 12-105 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		

Table 12-105 MvrSiteDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 12-106 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 12-107 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		

Table 12-107 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 12-108 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 12-109 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 12-110 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 12-111 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 12-112 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		

Table 12-112 NodeSuspended (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 12-113 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 12-114 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 12-115 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 12-116 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 12-117 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-117 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 12-118 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 12-119 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 12-120 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-121 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-122 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		

Table 12-122 PeerLacIngressEgressFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 12-123 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 12-124 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.0.0 • 9.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 12-125 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 12-126 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 12-127 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 12-127 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 12-128 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-129 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-130 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-131 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-132 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		

Table 12-132 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 12-133 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-134 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-135 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 12-136 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 12-137 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		

Table 12-137 PrimaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 12-138 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 12-139 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 12-140 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 12-141 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 12-142 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		

Table 12-142 PTPReferenceOutOfFrequency (sonet) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 12-143 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPol-lInRange	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 12-144 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 12-145 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 12-146 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 12-147 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 12-148 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 12-149 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		

Table 12-149 RouteDistinguisherNotConfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 12-150 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 12-151 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 12-152 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 12-153 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 12-154 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		

Table 12-154 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 12-155 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 12-156 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 12-157 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 12-158 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 12-159 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		

Table 12-159 ShamLinkDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 12-160 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 12-161 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 12-162 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 12-163 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 12-164 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		

Table 12-164 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 12-165 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 12-166 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 12-167 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 12-168 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 12-169 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		

Table 12-169 TPLSPDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 12-170 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 12-171 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 12-172 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 12-173 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		

Table 12-173 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 12-174 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 12-175 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 12-176 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 12-177 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 12-178 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		

Table 12-178 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 12-179 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 12-180 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 12-181 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 12-182 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 12-183 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		

Table 12-183 UplinkPartiallyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 12-184 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 12-185 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 12-186 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 12-187 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 12-188 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 12-189 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

13 7210 SAS-X

13.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 13-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 13-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 13-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 13-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 13-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 13-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 13-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 13-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 13-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 13-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 13-11 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 13-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 13-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-13 BfdInterfaceConnectionDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 13-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 13-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 13-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 13-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-18 BITS2ReferenceOutOfFrequency (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 13-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 13-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 13-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 13-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 13-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-23 BITSReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 13-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 13-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 13-25 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 13-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 13-27 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		

Table 13-27 CircuitStpExceptionCondition (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 13-28 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 13-29 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 13-30 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 13-31 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 13-32 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 13-33 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 13-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 13-35 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 13-36 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 13-37 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 13-38 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-38 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 13-39 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-40 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		

Table 13-40 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 13-41 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 13-42 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 13-43 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 13-44 EthernetPortCrcFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortCrcFailure (3629) Type: communicationsAlarm Package: ethernetequipment.EthernetPortCrcFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortCrcFailure	Release: • 7.0.0 • 8.0.0
Description: The alarm is raised when an Ethernet port CRC alarm condition is detected (Signal Degradation Threshold or Signal Failure Threshold exceeded).		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 13-45 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-45 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 13-46 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 13-47 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		

Table 13-47 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 13-48 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 13-49 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 13-50 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 13-51 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 13-52 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 13-53 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 13-54 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 13-55 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 13-56 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-56 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 13-57 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 13-58 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		

Table 13-58 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 13-59 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 13-60 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 13-61 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 13-62 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 13-63 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 13-64 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 13-65 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 13-66 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 13-67 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-67 inSufficientBandwidth (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 13-68 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 13-69 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		

Table 13-69 InterfaceNeighborDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-70 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 13-71 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 13-72 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 13-73 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 13-74 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 13-75 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 13-76 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 13-77 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 13-78 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-78 LdpSessionNonexistent (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 13-79 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 13-80 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 13-81 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 13-82 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 13-83 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 13-84 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 13-85 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 13-86 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 13-87 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-87 macMoveRateExceeded (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 13-88 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 13-89 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 13-89 MCLagDown (lag) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 13-90 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 13-91 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 13-92 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 13-93 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 13-94 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 13-95 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 13-96 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		

Table 13-96 MvrConfiguredProxySapNotExist (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 13-97 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 13-98 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-99 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 13-100 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 13-101 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 13-102 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 13-103 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 13-104 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 13-105 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		

Table 13-105 nonDeployedAdjacencyExists (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 13-106 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 13-107 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-108 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 13-109 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 13-110 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 13-111 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 13-112 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-113 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-114 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 13-115 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 13-116 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 13-117 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 13-118 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-118 PortEtherSymMonSDAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 13-119 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 13-120 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		

Table 13-120 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-121 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-122 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-123 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-124 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 13-125 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-126 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-127 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 13-128 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 13-129 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 13-130 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 13-131 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 13-132 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 13-133 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 13-134 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 13-135 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-135 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 13-136 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 13-137 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 13-137 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 13-138 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 13-139 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 13-140 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 13-141 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 13-142 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 13-143 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 13-144 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-144 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 13-145 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 13-146 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		

Table 13-146 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 13-147 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 13-148 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 13-149 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 13-150 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 13-151 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 7.0.0 • 8.0.0 • 9.0.0

Table 13-151 ShamLinkDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-152 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 13-153 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 13-154 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 13-155 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 13-156 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-156 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 13-157 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 13-158 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 13-159 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 13-160 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 13-161 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 13-162 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 13-162 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 13-163 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 13-164 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 13-165 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 13-166 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-166 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 13-167 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 13-168 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 13-169 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 13-170 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 13-171 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0

Table 13-171 upgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 13-172 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 13-173 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 13-174 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 13-175 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-176 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 13-177 VwmShelfCardIdMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfCardIdMismatch (5660) Type: equipmentAlarm Package: equipment.VwmShelfCardIdMismatch Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardIdMismatch	Release: • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the configured vwm card id is different than the equipped vwm card.		
Raising condition: ('administrativeState' EQUAL 'Up')		
Clearing condition: (('Assigned VWM Card Type' EQUAL 'Not Provisioned') OR ('Assigned VWM Card Type' EQUAL 'Not Equipped') OR ('administrativeState' EQUAL 'Down'))		
Remedial action: This alarm is raised when the detected VWM shelf card id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 13-178 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 13-179 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 5.0.0 • 6.0.0 • 7.0.0 • 8.0.0 • 9.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

14 7450 ESS

14.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 14-1 AaPolicerResourcesExceeded

Alarm	Attributes	Applicable major release
Name: AaPolicerResourcesExceeded (2930) Type: configurationAlarm Package: aapolicy.AaPolicerResourcesExceeded Raised on class: aapolicy.AaSubOvrd	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AaPolicerResourcesExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Application Assurance configured override values exceed policer resources.		
Raising condition: (('Policer Resource Status' EQUAL 'Exceeded'))		
Clearing condition: (('Policer Resource Status' NOT EQUAL 'Exceeded'))		
Remedial action: The Application Assurance Subscriber Policy override(s) configuration has exceeded the policer resources. Remove overrides of a policy configuration for an Application Assurance subscriber where this may be occurring. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-2 AarpDown

Alarm	Attributes	Applicable major release
Name: AarpDown (3704) Type: AarpDown Package: aapolicy.AarpDown Raised on class: aapolicy.Aarp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aarpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an AARP is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 14-2 AarpDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The application assurance redundancy protocol is down either because it is administratively disabled, faulty or a peer address is not up. Ensure that the AARP is administratively up, and the peer ip address and this ip address points to each other.		

Table 14-3 AarpInterfaceDown

Alarm	Attributes	Applicable major release
Name: AarpInterfaceDown (3904) Type: AarpInterfaceDown Package: service.AarpInterfaceDown Raised on class: service.AarpInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an AARP interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 14-4 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		

Table 14-4 AccessInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 14-5 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 14-6 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 14-7 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 14-8 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 14-9 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 14-10 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 14-11 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 14-12 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 14-13 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-13 AuthKeyConflict (rsvp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 14-14 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 14-15 BackPlaneEPROMFailed

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMFailed (12488) Type: equipmentAlarm Package: netw.BackPlaneEPROMFailed Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access the backplane EPROM due to a hardware defect.		
Remedial action: The active CPM is at risk of failing to initialize after node reboot due to not being able to access the BP EPROM to read the chassis type. Contact Nokia customer support.		

Table 14-16 BackPlaneEPROMWarning

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMWarning (12489) Type: equipmentAlarm Package: netw.BackPlaneEPROMWarning Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access one backplane EPROM due to a hardware defect but a redundant EPROM is present and accessible.		
Remedial action: There is no effect on system operation.No recovery action required.		

Table 14-17 backupScriptInUse

Alarm	Attributes	Applicable major release
Name: backupScriptInUse (274) Type: configurationAlarm Package: subscrident.backupScriptInUse Raised on class: subscrident.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupInUse	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary subscriber identification script is operationally down, but one of the other scripts is operationally up.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND (('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR (('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 14-18 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-18 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 14-19 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 14-20 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		

Table 14-20 BerLineSignalFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 14-21 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 14-22 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 14-23 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 14-24 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-25 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-25 BITS2NotQualified (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 14-26 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 14-27 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 14-28 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 14-29 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 14-30 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-30 BITSReferenceLossOfSignal (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 14-31 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 14-32 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 14-33 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 14-34 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 14-35 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 14-36 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 14-37 CcagDown

Alarm	Attributes	Applicable major release
Name: CcagDown (210) Type: equipmentAlarm Package: ccag.CcagDown Raised on class: ccag.CrossConnectAggregationGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CcagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the CCAG Administrative State is Up and the Operational State is Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 14-38 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-39 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-39 CesBfrUnderrun (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-40 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-41 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-42 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-43 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-44 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-45 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 14-46 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 14-47 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 14-48 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 14-49 CoherentOpticalModuleFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleFault (4612) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ModuleFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports module fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault')))		
Remedial action: Module Fault occurred.		

Table 14-50 CoherentOpticalModuleHostTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleHostTxFault (4613) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleHostTxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleHostTxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Host Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit'))		

Table 14-50 CoherentOpticalModuleHostTxFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit')))		
Remedial action: Module Host Tx Fault occurred.		

Table 14-51 CoherentOpticalModuleReferenceLockLoss

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleReferenceLockLoss (4614) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleReferenceLockLoss Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceLockLoss	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports loss of reference lock signal on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module')))		
Remedial action: Loss of reference lock.		

Table 14-52 CoherentOpticalModuleRxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleRxFault (4615) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleRxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleRxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Rx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive')))		
Remedial action: Module Rx Fault occurred.		

Table 14-53 CoherentOpticalModuleTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleTxFault (4616) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleTxFault Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleTxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit')))		
Remedial action: Module Tx Fault occurred.		

Table 14-54 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 14-55 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		

Table 14-55 ConfigurationRescueFileSaveStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 14-56 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 14-57 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 14-58 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback.ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 14-59 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 14-60 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 14-61 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 14-62 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 14-63 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		

Table 14-63 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 14-64 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 14-65 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 14-65 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 14-66 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-67 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-68 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-69 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtViolPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-70 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-70 CpmProtectionViolationSAPEntry (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-71 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 14-72 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 14-73 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec.CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 14-74 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-75 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		

Table 14-75 DDMAux1HighWarning (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-76 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-77 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-78 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-79 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-80 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-80 DDMAux2LowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-81 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-82 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-83 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-84 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-85 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-85 DDMRxOpticalPowerLowWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-86 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-87 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-88 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-89 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-90 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-90 DDMTemperatureHighAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-91 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-92 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-93 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-94 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-95 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-95 DDMTxBiasCurrentHighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-96 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-97 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-98 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-99 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-100 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-100 DDMTxOutputPowerLowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-101 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 14-102 DeterministicNatMapOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatMapOperDown (9570) Type: equipmentAlarm Package: nat.DeterministicNatMapOperDown Raised on class: nat.DeterministicNatMap	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatMapOper-Down	Release: • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Map is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 14-103 DeterministicNatPrefixOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatPrefixOperDown (9571) Type: equipmentAlarm Package: nat.DeterministicNatPrefixOperDown Raised on class: nat.DeterministicNatPrefix	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatPrefixOper-Down	Release: • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Prefix is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'InService') AND ('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 14-104 DhcpLseStateMobilityError

Alarm	Attributes	Applicable major release
Name: DhcpLseStateMobilityError (8409) Type: configurationAlarm Package: service.DhcpLseStateMobilityError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapDHCPLseStateMobilityEr-ror	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system was unable to perform a mobility check for this lease state.		
Remedial action: Please make sure that host-connectivity-verify is enabled on the SAP.		

Table 14-105 DhcpLseStateRestoreProblem

Alarm	Attributes	Applicable major release
Name: DhcpLseStateRestoreProblem (8402) Type: processingErrorAlarm Package: netw.DhcpLseStateRestoreProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpLseStateRestoreProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when an error is detected while processing a persistency record.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 14-106 DhcpMiscellaneousProblem

Alarm	Attributes	Applicable major release
Name: DhcpMiscellaneousProblem (8403) Type: processingErrorAlarm Package: netw.DhcpMiscellaneousProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpMiscellaneousProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a miscellaneous DHCP problem occurs.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 14-107 DHCPPoolFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPPoolFailoverStateChange (5168) Type: configurationAlarm Package: dhcp.DHCPPoolFailoverStateChange Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPPoolFailoverStat-eChanged	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Local DHCP Pool Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when the operational state of a particular Local DHCP Pool Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a pool failover is in progress.\nThis alarm is cleared implicitly when the DHCP Pool Failover state returns to Normal.		

Table 14-108 DHCPServerFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPServerFailoverStateChange (4986) Type: configurationAlarm Package: dhcp.DHCPServerFailoverStateChange Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPServerFailoverStat-eChanged	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Local DHCP Server Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		

Table 14-108 DHCPServerFailoverStateChange (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when operational state of a particular Local DHCP Server Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a server failover is in progress.\nThis alarm will be cleared implicitly when the DHCP Server Failover state returns to Normal.		

Table 14-109 DHCPSFoLeaseUpdateFailedAddressConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedAddressConflict (4977) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedAddressConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedAddressConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a address conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased another address to this host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased another address to this host. Please ensure all configuration is correct.		

Table 14-110 DHCPSFoLeaseUpdateFailedfoShutdown

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedfoShutdown (4985) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedfoShutdown Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedfoShutdown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a shutdown lease update received from the failover peer cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'. Please ensure all configuration is correct.		

Table 14-111 DHCPSFoLeaseUpdateFailedHostConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedHostConflict (4978) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedHostConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedHostConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a host conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased this address to another host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased this address to another host. Please ensure all configuration is correct.		

Table 14-112 DHCPSFoLeaseUpdateFailedLeaseExpired

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedLeaseExpired (4979) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedLeaseExpired Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedLeaseExpired	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a lease expired lease update received from the failover peer cannot be processed successfully. The lease received from the peer has expired.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer has expired. Please ensure all configuration is correct.		

Table 14-113 DHCPSFoLeaseUpdateFailedMaxLeaseReached

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedMax-LeaseReached (4980) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedMaxLeaseReached Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedMaxLeaseReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a maximum reached lease update received from the failover peer cannot be processed successfully. The maximum number of leases is already reached.		

Table 14-113 DHCPSFoLeaseUpdateFailedMaxLeaseReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The maximum number of leases is already reached. Please ensure all configuration is correct.		

Table 14-114 DHCPSFoLeaseUpdateFailedPeerConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPeerConflict (4981) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPeerConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPeerConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a peer conflict lease update received from the failover peer cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance. Please ensure all configuration is correct.		

Table 14-115 DHCPSFoLeaseUpdateFailedPersistenceCongested

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPer-sistenceCongested (4982) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPersistenceCongested Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPersistenceCongested	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a persistence congested lease update received from the failover peer cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload. Please ensure all configuration is correct.		

Table 14-116 DHCPSFoLeaseUpdateFailedRangeNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedRangeNotFound (4983) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedRangeNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFaile-dRangeNotFound	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a range not found lease update received from the failover peer cannot be processed successfully. No valid include range for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid include range for this lease could be found. Please ensure all configuration is correct.		

Table 14-117 DHCPSFoLeaseUpdateFailedSubnetNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedSubnetNotFound (4984) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedSubnetNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedSubnetNotFound	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a subnet not found lease update received from the failover peer cannot be processed successfully. No valid subnet for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid subnet for this lease could be found. Please ensure all configuration is correct.		

Table 14-118 DhcpSvrNoSubnetFixAddr

Alarm	Attributes	Applicable major release
Name: DhcpSvrNoSubnetFixAddr (8378) Type: configurationAlarm Package: dhcp.DhcpSvrNoSubnetFixAddr Raised on class: dhcp.LocalDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpSvrNoSubnetFixAddr	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm can be generated for hosts configured with a fixed IP address in the local user database. If such a host requests an ip-address and the system cannot find a matching subnet in this server instance for this IP address, then this alarm is generated, and the request is dropped.		

Table 14-118 DhcpSvrNoSubnetFixAddr (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that the IP Address configured for this host under the local user database falls into a subnet under the local DHCP server mapped to this alarm.		

Table 14-119 DiamAppMessageDropped

Alarm	Attributes	Applicable major release
Name: DiamAppMessageDropped (5175) Type: processingErrorAlarm Package: diameter.DiamAppMessageDropped Raised on class: diameter.DiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamAppMessageDropped	Release: • 12.0 • 13.0
Description: The alarm is raised when the Diameter protocol has dropped a message		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 14-120 DiamProxyOperationalStateChange

Alarm	Attributes	Applicable major release
Name: DiamProxyOperationalStateChange (8427) Type: communicationsAlarm Package: diameter. DiamProxyOperationalStateChange Raised on class: diameter.DiameterPeerProxy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiameterProxyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Diameter Peer Proxy is Out Of Service.		
Raising condition: ('Operational State' EQUAL 'Out Of Service')		
Clearing condition: ('Operational State' EQUAL 'in Service')		
Remedial action: Please ensure that the Diameter Peer Proxy on Diameter Policy is operationally up.		

Table 14-121 DiscoveredPhysicalLinkMismatch

Alarm	Attributes	Applicable major release
Name: DiscoveredPhysicalLinkMismatch (657) Type: configurationAlarm Package: netw.DiscoveredPhysicalLinkMismatch Raised on class: netw.AbstractPhysicalLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: endPointUsedByNumerou-sLinks	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one endpoint of a physical link is used as an endpoint in another physical link.		
Raising condition: ('physicalLinkMismatchConfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMismatchConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. Physical link endpoint (i.e. ports) can only be configured in one link.		

Table 14-122 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 14-123 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 14-124 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 14-125 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 14-126 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 14-127 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment.DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-127 DS1E1ResourceAvailabilityIndicator (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 14-128 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 14-129 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 14-130 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 14-131 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 14-132 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 14-133 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 14-134 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-134 DS3E3ResourceAvailability (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 14-135 DuplicatePhysicalLinks

Alarm	Attributes	Applicable major release
Name: DuplicatePhysicalLinks (658) Type: configurationAlarm Package: netw.DuplicatePhysicalLinks Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicatePhysicalLinkConfig-ured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is more then one physical link configured between two endpoints.		
Raising condition: ('duplicateLinkConfigured' EQUAL 'true')		
Clearing condition: ('duplicateLinkConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The duplicated link must be deleted.		

Table 14-136 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		

Table 14-136 EfmOamAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 14-137 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 14-138 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 14-139 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 14-140 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-141 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 14-142 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 14-143 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-143 EquipmentRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 14-144 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 14-145 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 14-146 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 14-147 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 14-148 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 14-149 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 14-150 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 14-151 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 14-152 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 14-153 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 14-154 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 14-155 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 14-156 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-156 FanTrayRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 14-157 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 14-158 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		

Table 14-158 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 14-159 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 14-160 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 14-161 GRETunnelDown

Alarm	Attributes	Applicable major release
Name: GRETunnelDown (3326) Type: serviceAlarm Package: svt.GRETunnelDown Raised on class: svt.GRETunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IP/GRE tunnel Operational State changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The situation may occur if the underlying physical port is down either because of administrative disabling or a fault on the port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable.		

Table 14-162 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 14-163 GroupInterfaceDown

Alarm	Attributes	Applicable major release
Name: GroupInterfaceDown (441) Type: GroupInterfaceAlarm Package: service.GroupInterfaceDown Raised on class: service.GroupInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-163 GroupInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects that a group interface is operationally down. The alarm clears when the group interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 14-164 HostConnectivityLostRateExceeded

Alarm	Attributes	Applicable major release
Name: HostConnectivityLostRateExceeded (276) Type: communicationsAlarm Package: ressubscr. HostConnectivityLostRateExceeded Raised on class: ressubscr.ShcvSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hostDown Applicable probable causes: • hostDown • trapDropped	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the trapDroppedRaisesAlarm parameter is enabled and the maximum allowed number of SHCV host connectivity loss events on a SAP is exceeded. The SHCV action in response to the alarm is specified by the maxHostLostConnectivityRate parameter. If the specified action is to remove the host information, the host information is removed and the connectivity of the host is not subsequently verified.		
Remedial action: This may be a transient error condition in the network or possible congestion or could be a sign that the SHCV ping interval is too short. Verify the status of the network for those subscribers and the service SHCV configuration.		

Table 14-165 IGHMisconfigured

Alarm	Attributes	Applicable major release
Name: IGHMisconfigured (827) Type: ighAlarm Package: igh.IGHMisconfigured Raised on class: igh.InterfaceGroupHandler	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IGHProtocolMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IGH is administratively up but none of the IGH protocols is operationally up.		
Raising condition: (('igh_misconfigured' EQUAL '\"yes\"') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('igh_misconfigured' NOT EQUAL '\"yes\"') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Please check the configuration.		

Table 14-166 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 14-167 IgmpMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxGrpSrcsLimitExceeded (4624) Type: configurationAlarm Package: igmp.IgmpMaxGrpSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Needs to increase 'maxGrpSources' value to allow more sources on this interface.		

Table 14-168 IgmpMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxSrcsLimitExceeded (3742) Type: configurationAlarm Package: igmp.IgmpMaxSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxSrcsLimitExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP source for a group when the number of sources for this group is equal to 'maxSources', the maximum number of sources per group supported on the interface.		
Remedial action: Needs to increase 'maxSources' value to allow more sources on this interface.		

Table 14-169 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 14-170 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 14-171 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 14-172 IncorrectNeighborConfig

Alarm	Attributes	Applicable major release
Name: IncorrectNeighborConfig (609) Type: configurationAlarm Package: aps.IncorrectNeighborConfig Raised on class: aps.ApsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incorrectNeighborConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.		
Raising condition: (('Type' EQUAL 'MultiChassis') AND ('Neighbor match' EQUAL 'false'))		
Clearing condition: (('Type' EQUAL 'SingleChassis') OR ('Neighbor match' EQUAL 'true'))		
Remedial action: Make sure a peer exist and the neighbor address points to a network interface on the NE that contains the peer object.		

Table 14-173 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 14-174 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 14-175 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 14-176 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 14-177 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-177 InstanceDown (vrrp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 14-178 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 14-179 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 14-180 InterfaceDown (service)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: service.InterfaceDown Raised on class: service.RedundantInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a redundant interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 14-181 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 14-182 InterfaceDown (vprn)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vprn.InterfaceDown Raised on class: vprn.IPMirrorInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 14-183 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-184 IOMEventOverflow

Alarm	Attributes	Applicable major release
Name: IOMEventOverflow (5617) Type: equipmentAlarm Package: equipment.IOMEventOverflow Raised on class: equipment.BaseCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMEventOverflow	Release: • 12.0 • 13.0 • 14.0

Table 14-184 IOMEventOverflow (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is generated when tmnxIomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimitReached occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.		
Remedial action: Informational - The alarm will be cleared when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.		

Table 14-185 IOMResUtilizationLimit

Alarm	Attributes	Applicable major release
Name: IOMResUtilizationLimit (5618) Type: equipmentAlarm Package: equipment.IOMResUtilizationLimit Raised on class: equipment.BaseCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMResHighLimitReached Applicable probable causes: • IOMResHighLimitReached • IOMResExhausted	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the value of tmnxIomResourceLimitPct.		
Remedial action: Informational - The alarm will be cleared when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.		

Table 14-186 IPSecGatewayDown

Alarm	Attributes	Applicable major release
Name: IPSecGatewayDown (830) Type: serviceAlarm Package: ipsec.IPSecGatewayDown Raised on class: ipsec.IPSecGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: gatewayDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a SAP IPsec gateway changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 14-187 IPSecIsaGrpDown

Alarm	Attributes	Applicable major release
Name: IPSecIsaGrpDown (3745) Type: equipmentAlarm Package: isa.IPSecIsaGrpDown Raised on class: isa.IPSecIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPSecIsaGrpDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA IPSec group is Down and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Tunnel Group is down, despite the administrative state being up. Check that the configured ISA-Tunnel Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application IPSec(Tunnel) Group.		

Table 14-188 IPSecIsaMemoryHigh

Alarm	Attributes	Applicable major release
Name: IPSecIsaMemoryHigh (11089) Type: thresholdCrossed Package: equipment.IPSecIsaMemoryHigh Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The Alarm is generated when the ISA card memory usage ratio has reached the high watermark ,which is measured by the number of phase 1 and phase 2 security associations (SAs).		
Remedial action: This alarm is raised when the ISA card memory usage ratio reaches the high watermark which is measured by the number of phase 1 and phase 2 security associations (SAs). The value used for the high watermark is 95% of the maximum number of SAs for the ISA Card. The alarm is cleared when the ISA card memory usage ratio reaches the low watermark.		

Table 14-189 IPSecIsaMemoryMax

Alarm	Attributes	Applicable major release
Name: IPSecIsaMemoryMax (11090) Type: thresholdCrossed Package: equipment.IPSecIsaMemoryMax Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-189 IPSecIsaMemoryMax (continued)

Alarm	Attributes	Applicable major release
Description: The Alarm is generated when the ISA card memory usage ratio has reached the Maximum which is measured by the number of phase 1 and phase 2 security associations (SAs).		
Remedial action: This alarm is raised when the ISA card memory usage ratio reaches the maximum value of security associations (SAs) associated with the ISA Card. This maximum value is measured by the number of phase 1 and phase 2 SAs. The alarm is cleared when the number of SAs reaches the low watermark.		

Table 14-190 IPSecTunnelBfdConnectionBroken

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionBroken Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 14-191 IPSecTunnelBfdConnectionDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 14-192 IPSecTunnelBfdConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm Package: ipsec. IPSecTunnelBfdConnectionPeerDetectsDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 14-193 IPSecTunnelDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelDown (834) Type: serviceAlarm Package: ipsec.IPSecTunnelDown Raised on class: ipsec.IPSecTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IPsec tunnel operational state changes to 'down' and the administrative state is 'up'.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 14-194 IsaAaGrpDown

Alarm	Attributes	Applicable major release
Name: IsaAaGrpDown (647) Type: equipmentAlarm Package: isa.IsaAaGrpDown Raised on class: isa.AaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an ISA-AA group Operational State is Down, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 14-194 IsaAaGrpDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-AA group is down, despite the administrative state being up. Check that the configured ISA-AA Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Assurance MDA.		

Table 14-195 IsaAaSubUnassigned

Alarm	Attributes	Applicable major release
Name: IsaAaSubUnassigned (836) Type: equipmentAlarm Package: isa.IsaAaSubUnassigned Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaSubUnassigned	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. The unassigned subscriber is treated as specified by the Operation Upon Failure parameter in the AA group. Recovery from this condition requires the removal and recreation of the AA subscriber when sufficient resources are available.		
Raising condition: (('Number of Unassigned ESM Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned SAP Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned Spoke SDP Subscribers' NOT EQUAL '0L'))		
Clearing condition: (('Number of Unassigned ESM Subscribers' EQUAL '0L') AND ('Number of Unassigned SAP Subscribers' EQUAL '0L') AND ('Number of Unassigned Spoke SDP Subscribers' EQUAL '0L'))		
Remedial action: The subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. Remove and recreate the AA subscriber when sufficient resources are available.		

Table 14-196 IsaLnsGrpDown

Alarm	Attributes	Applicable major release
Name: IsaLnsGrpDown (1119) Type: equipmentAlarm Package: isa.IsaLnsGrpDown Raised on class: isa.LnsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaLnsGrpDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA-LNS group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 14-196 IsaLnsGrpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is caused by administrative shutdown or equipment failure of the MDA members. Review the status of the underlying ISA MDA group members and ensure they are operational.		

Table 14-197 IsaVideoGrpDown

Alarm	Attributes	Applicable major release
Name: IsaVideoGrpDown (775) Type: equipmentAlarm Package: isa.IsaVideoGrpDown Raised on class: isa.VideoGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaVideoGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA video group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Video Group is down, despite the administrative state being up. Check that the configured ISA-Video Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Video Group.		

Table 14-198 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 14-199 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 14-200 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 14-201 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-201 KeepAliveProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 14-202 L2TPDown

Alarm	Attributes	Applicable major release
Name: L2TPDown (841) Type: ProtocolAlarm Package: l2tp.L2TPDown Raised on class: l2tp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2TP site becomes administratively down. The alarm clears when the L2TP site becomes administratively up.		
Raising condition: ('Administrative State' EQUAL 'Down')		
Clearing condition: ('Administrative State' EQUAL 'Up')		
Remedial action: This alarm indicates that the L2TP protocol administrative state is down. It is cleared automatically when L2TP administrative state is up again. Please verify the L2TP configuration. This alarm can be safely suppressed if L2TP is not used.		

Table 14-203 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		

Table 14-203 LabelProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 14-204 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 14-205 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 14-206 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 14-207 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 14-208 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-208 LdpTargetedPeerDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 14-209 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 14-210 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		

Table 14-210 LineAlarmIndicationSignal (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 14-211 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-212 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 14-213 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 14-214 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 14-215 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 14-216 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 14-217 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment.LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 11.0 • 12.0

Table 14-217 LowTemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 14-218 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 14-219 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		

Table 14-219 LspPathBypassTunnelActive (continued)

Alarm	Attributes	Applicable major release
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 14-220 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 14-221 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 14-222 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 14-223 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 14-224 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-224 macMoveRateExceededNonBlock (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 14-225 McIPsecPeerTunnelGroupMissing

Alarm	Attributes	Applicable major release
Name: McIPsecPeerTunnelGroupMissing (4815) Type: configurationAlarm Package: multichassis. McIPsecPeerTunnelGroupMissing Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC IPsec tunnel group. This can be either the peer tunnel group is misconfigured or the local peer group ID is not configured.		
Raising condition: ('peerTunnelGroupPointer' EQUAL '\"\"')		
Clearing condition: ('peerTunnelGroupPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC IPsec tunnel group or check the local tunnel group's peer group ID has been configured, or delete this one if it is not used.		

Table 14-226 McIPsecTunnelGroupDown

Alarm	Attributes	Applicable major release
Name: McIPsecTunnelGroupDown (4816) Type: redundancyAlarm Package: multichassis.McIPsecTunnelGroupDown Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipsecTunnelGroupDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MC IPsec tunnel group is operationally down while it is administratively up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check if the physical ISA IPsec Tunnel Group or the associated MDA is operationally down.		

Table 14-227 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 14-228 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 14-229 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC endpoint is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 14-230 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 14-231 MepFacilityFault (lag)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: lag.MepFacilityFault Raised on class: lag.Interface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-231 MepFacilityFault (lag) (continued)

Alarm	Attributes	Applicable major release
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 14-232 MepFacilityFault (rtr)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: rtr.MepFacilityFault Raised on class: rtr.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 14-233 MepFacilityFault (equipment)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: equipment.MepFacilityFault Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 14-234 MepFacilityFault (service)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: service.MepFacilityFault Raised on class: service.AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 14-235 MigrationCompleted

Alarm	Attributes	Applicable major release
Name: MigrationCompleted (753) Type: migrationComplete Package: equipment.MigrationCompleted Raised on class: equipment.NeCardSwapTask	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationComplete	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a card migration event completes.		
Raising condition: ('Status' EQUAL 'Migration completed')		
Remedial action: Informational - no corrective action required.		

Table 14-236 MigrationFailed

Alarm	Attributes	Applicable major release
Name: MigrationFailed (754) Type: migrationFailure Package: equipment.MigrationFailed Raised on class: equipment.NeCardSwapTask	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a card migration event fails.		

Table 14-236 MigrationFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Status' EQUAL 'Failed - Latest configuration not available') OR ('Status' EQUAL 'Failed - Unable to migrate configuration') OR ('Status' EQUAL 'Failed - Unable to transfer migrated configuration') OR ('Status' EQUAL 'Failed - Unable to reboot network element'))		
Remedial action: This alarm is raised when a card migration fails. The operation has failed for one of the following reasons - a configuration backup could not be created, the configuration transfer failed or the attempt to reboot the card failed. Please re-attempt the migration. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-237 MinFreePfxThDepleted

Alarm	Attributes	Applicable major release
Name: MinFreePfxThDepleted (9032) Type: configurationAlarm Package: dhcp.MinFreePfxThDepleted Raised on class: dhcp.PrefixMinFreeThreshold	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix becomes zero.		
Remedial action: The operator may create additional prefixes in the considered prefix. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 14-238 MinFreePfxThTooLow

Alarm	Attributes	Applicable major release
Name: MinFreePfxThTooLow (9033) Type: configurationAlarm Package: dhcp.MinFreePfxThTooLow Raised on class: dhcp.PrefixMinFreeThreshold	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesTooLow	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix is becoming too low.		
Remedial action: The operator may create additional prefixes in the considered prefix to prevent a shortage of available prefixes with minimum free threshold length. \nAlternatively, examination of the leases in the prefix may reveal that the distribution is not appropriate.		

Table 14-239 MinFreePoolThDepleted

Alarm	Attributes	Applicable major release
Name: MinFreePoolThDepleted (9034) Type: configurationAlarm Package: dhcp.MinFreePoolThDepleted Raised on class: dhcp.AddressPoolMinFreeThreshold	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the pool becomes zero.		
Remedial action: The operator may create additional prefixes in the pool. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 14-240 MinFreePoolThTooLow

Alarm	Attributes	Applicable major release
Name: MinFreePoolThTooLow (9035) Type: configurationAlarm Package: dhcp.MinFreePoolThTooLow Raised on class: dhcp.AddressPoolMinFreeThreshold	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesTooLow	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the pool is becoming too low.		
Remedial action: Please create additional prefixes in the pool to prevent a shortage of available prefixes with minimum free threshold length. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 14-241 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		

Table 14-241 MissingLocalEntry (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 14-242 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 14-243 MldMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxGrpSrcsLimitExceeded (5395) Type: configurationAlarm Package: mld.MldMaxGrpSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an MLD group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Increase the value of the 'Maximum Number of Group Sources' attribute in the parent MLD interface so that the number of active MLD group sources stays under the configured threshold.		

Table 14-244 MldMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxSrcsLimitExceeded (5396) Type: configurationAlarm Package: mld.MldMaxSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxSrcsLimitExceeded	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an MLD source for a group when the number of sources for this group is equal to 'maxSources', the Maximum Number of Sources per group supported on the interface.		
Remedial action: Increase 'Maximum Number Of Sources' value to allow more sources on this interface.		

Table 14-245 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 14-246 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 14-246 MplsDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 14-247 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 14-248 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		

Table 14-248 MrpAttrTblSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 14-249 MsdpDown

Alarm	Attributes	Applicable major release
Name: MsdpDown (353) Type: ProtocolAlarm Package: msdp.MsdpDown Raised on class: msdp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the MSDP site.		

Table 14-250 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 14-251 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 14-252 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 14-253 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 14-254 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 14-255 NatDeterministicChange

Alarm	Attributes	Applicable major release
Name: NatDeterministicChange (5122) Type: configurationAlarm Package: netw.NatDeterministicChange Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatDeterministicMapChanged	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when something changed in the Deterministic NAT map. Such a change may be caused by a modification of the Deterministic NAT Prefix or the Deterministic NAT Map.		

Table 14-255 NatDeterministicChange (continued)

Alarm	Attributes	Applicable major release
Remedial action: Managers that rely on the offline representation of the Deterministic NAT map should get an updated copy by saving the Deterministic NAT script.		

Table 14-256 NatIsaGrpDegraded

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDegraded (8059) Type: equipmentAlarm Package: nat.NatIsaGrpDegraded Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDegraded	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the NAT ISA group is degraded, while operationally still in service.		
Raising condition: (('Degraded State' EQUAL 'True') AND ('Operational State' EQUAL 'Up'))		
Clearing condition: (('Operational State' NOT EQUAL 'Up') OR ('Degraded State' NOT EQUAL 'True'))		
Remedial action: The ISA-NAT Group is degraded. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 14-257 NatIsaGrpDown

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDown (3887) Type: equipmentAlarm Package: nat.NatIsaGrpDown Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an NAT ISA group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-NAT Group is down, despite the administrative state being up. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 14-258 NatIsaMemberSessionUsageHi

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHi (3937) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHi Raised on class: nat.IsaMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-259 NatIsaMemberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHigh (1070) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHigh Raised on class: nat.IsaMda	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Deprecated in 10.0, Use {NatIsaMemberSessionUsageHi on nat.IsaMember} instead. The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-260 NatLsnSubscriberIcmpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsageHigh (4860) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-261 NatLsnSubscriberIcmpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsgHigh (5397) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-262 NatLsnSubscriberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsageHigh (4861) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 14-263 NatLsnSubscriberSessionUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsgHigh (5398) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 14-264 NatLsnSubscriberTcpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsageHigh (4862) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-265 NatLsnSubscriberTcpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsgHigh (5399) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-266 NatLsnSubscriberUdpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsageHigh (4863) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-267 NatLsnSubscriberUdpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsgHigh (5400) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 14-268 NatMdaDetectsLoadSharingError

Alarm	Attributes	Applicable major release
Name: NatMdaDetectsLoadSharingError (5120) Type: configurationAlarm Package: nat.NatMdaDetectsLoadSharingError Raised on class: nat.IsaMda	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatMdaLoadSharingErrorDetected	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when node is sending periodically at most every 10 seconds while a NAT ISA MDA detects that it is receiving packets erroneously, due to incorrect load-balancing by the ingress IOM. The MDA drops all incorrectly load-balanced traffic.		
Remedial action: The ingress IOM hardware does not support a particular NAT function's load-balancing, for example an IOM-2 does not support deterministic NAT. Upgrade the ingress IOM, or change the configuration.		

Table 14-269 NatPcpSrvStateDown

Alarm	Attributes	Applicable major release
Name: NatPcpSrvStateDown (4382) Type: communicationsAlarm Package: nat.NatPcpSrvStateDown Raised on class: nat.PcpServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatPcpSrvStateDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an NAT PCP Server Changes		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates the PCP Server Operational State is Down.\n Please check the State Description on the PCP server for detail information		

Table 14-270 NatPlL2AwBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlL2AwBlockUsageHigh (1074) Type: equipmentAlarm Package: nat.NatPlL2AwBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the block usage of an L2-aware NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		
Remedial action: This alarm indicates the block usage of a L2-aware NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 14-271 NatPlLsnMemberBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlLsnMemberBlockUsageHigh (1075) Type: equipmentAlarm Package: nat.NatPlLsnMemberBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the block usage of a large-scale NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		
Remedial action: This alarm indicates the block usage of a Large Scale NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 14-272 NatResourceProblem

Alarm	Attributes	Applicable major release
Name: NatResourceProblem (9575) Type: equipmentAlarm Package: netw.NatResourceProblem Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: natResourceProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-272 NatResourceProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when resource problem is detected while attempting to activate some part of the NAT configuration of a system		
Remedial action: A resource problem was detected while attempting to activate a component of the system NAT configuration. Make sure the ISA card on the NE has sufficient resources available.		

Table 14-273 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-274 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 14-274 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 14-275 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 14-276 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-276 NodeDatabaseFallbackDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 14-277 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 14-278 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 14-279 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 14-280 noFunctioningScript

Alarm	Attributes	Applicable major release
Name: noFunctioningScript (275) Type: configurationAlarm Package: subscrident.noFunctioningScript Raised on class: subscrident.Policy	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryBackupDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all subscriber identification scripts are operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND ('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR ('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 14-281 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 14-282 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 14-283 NoSFMConfigured

Alarm	Attributes	Applicable major release
Name: NoSFMConfigured (11179) Type: equipmentAlarm Package: netw.NoSFMConfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoSFMConfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-283 NoSFMConfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when none of the SFM are configured.		
Remedial action: This alarm indicates that none of the SFM is configured. Please configured a SFM.		

Table 14-284 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 14-285 ObsoleteProtocolInFilter

Alarm	Attributes	Applicable major release
Name: ObsoleteProtocolInFilter (3706) Type: ConfigurationAlarm Package: aapolicy.ObsoleteProtocolInFilter Raised on class: aapolicy.ApplicationFilter	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: obsoleteProtocolInFilter	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a local application filter refers to an obsolete application assurance protocol.		
Remedial action: Change the application filter configuration to use a protocol that is not Obsolete.		

Table 14-286 OFFlowEntryDeploymentCreateFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentCreateFailed (5405) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentCreateFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentCreateFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Creation Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Creation Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects creation of the flow.		

Table 14-287 OFFlowEntryDeploymentDeleteFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentDeleteFailed (5406) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentDeleteFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentDeleteFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Deletion Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Deletion Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects deletion of the flow.		

Table 14-288 OFLogicalPortStatusMplsTpNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusMplsTpNotSet (5407) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusMplsTpNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusMplsTpNotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the MPLS-TP flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'rsvp-te'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'rsvp-te'))		
Remedial action: When MPLS-TP is not set, OpenFlow port status will not be received by SAM.		

Table 14-289 OFLogicalPortStatusRsvpTeNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusRsvpTeNotSet (5408) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusRsvpTeNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusRs-vpTeNotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RSVP-TE flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'mpls-tp'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'mpls-tp'))		
Remedial action: When RSVP-TE is not set, OpenFlow port status will not be received by SAM.		

Table 14-290 OFSwitchDown

Alarm	Attributes	Applicable major release
Name: OFSwitchDown (5409) Type: equipmentAlarm Package: openflow.OFSwitchDown Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFSwitchDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an OFSwitch is Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is raised when the OpenFlow switch has gone down.		

Table 14-291 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		

Table 14-291 OspfInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-292 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 14-293 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		

Table 14-293 P2MPLSPDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 14-294 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 14-295 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 14-296 PccRuleInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: PccRuleInsertedFltrEntryDropped (11059) Type: configurationAlarm Package: aclfilter.PccRuleInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a request to insert a filter entry is not successful for a PCC rule application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for PCC rule application. Check the configuration filter entry.		

Table 14-297 PccRuleInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: PccRuleInsertSpaceThresholdAlarm (11058) Type: configurationAlarm Package: aclfilter.PccRuleInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a PCC rule application insert range.		
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for PCC rule application. Make an adjusted to the watermarks or to the filter.		

Table 14-298 PeerConnectionDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: msdp.PeerConnectionDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.		
Raising condition: (('connectionState' NOT EQUAL 'Established') AND ('administrativeState' EQUAL 'Up'))		

Table 14-298 PeerConnectionDown (msdp) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('connectionState' EQUAL 'Established') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Check the configurations of the peer routers.		

Table 14-299 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 14-300 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-301 PeerDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: msdp.PeerDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('administrativeState' EQUAL 'Down'))		
Clearing condition: (('administrativeState' NOT EQUAL 'Down'))		
Remedial action: Turn up the Peer.		

Table 14-302 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-303 PeerGroupDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: msdp.PeerGroupDown Raised on class: msdp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the Group.		

Table 14-304 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 14-305 PeerUnreachable

Alarm	Attributes	Applicable major release
Name: PeerUnreachable (842) Type: ProtocolAlarm Package: l2tp.PeerUnreachable Raised on class: l2tp.Peer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2TP peer becomes unreachable.		
Remedial action: This alarm is raised when L2TP peer is unreachable. Please verify the L2TP tunnel profile configuration to ensure that the peer is properly configured. Also verify that the peer is actually reachable from this network element. \nThis alarm is cleared automatically when L2TP Peer becomes reachable.		

Table 14-306 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 14-307 PhysicalLinkPortsMisconfigured

Alarm	Attributes	Applicable major release
Name: PhysicalLinkPortsMisconfigured (239) Type: configurationAlarm Package: netw.PhysicalLinkPortsMisconfigured Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: physicalLinkPortsMisconfig-ured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is an MTU size mismatch between a link endpoint and a port. The alarm clears when the MTUs match.		
Raising condition: ('physicalLinkMisconfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The MTU value(s) on the link endpoint and port must be changed such that they match.		

Table 14-308 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 14-309 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 14-310 PoolDepleted

Alarm	Attributes	Applicable major release
Name: PoolDepleted (3950) Type: configurationAlarm Package: dhcp.PoolDepleted Raised on class: dhcp.AddressPool	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Address pool becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a pool becomes zero. Please increase the pool address range or create another address pool.		

Table 14-311 PoolMinFreeExc

Alarm	Attributes	Applicable major release
Name: PoolMinFreeExc (3696) Type: configurationAlarm Package: dhcp.PoolMinFreeExc Raised on class: dhcp.AddressPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowPoolMin	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-311 PoolMinFreeExc (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		
Remedial action: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		

Table 14-312 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 14-313 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 14-314 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-315 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-316 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-316 PowerSupplyFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-317 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-318 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		

Table 14-318 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 14-319 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-320 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-321 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 14-322 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 14-323 PppoeNcpFailure

Alarm	Attributes	Applicable major release
Name: PppoeNcpFailure (8410) Type: processingErrorAlarm Package: service.PppoeNcpFailure Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapPppoeNcpFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates there is a NCP phase setup problem.		
Remedial action: This alarm indicates the NCP phase setup failed, thus IP protocol can not be configured for the user that attempted to set up the PPPoE session. Please verify NCP setup configuration.		

Table 14-324 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 14-325 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		

Table 14-325 PrimaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 14-326 ProxyMcLocalStateChange

Alarm	Attributes	Applicable major release
Name: ProxyMcLocalStateChange (9039) Type: communicationsAlarm Package: diameter.ProxyMcLocalStateChange Raised on class: diameter.DiameterPeerProxy	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProxyMcLocalStateChange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when proxyMcLocalState of a Diameter Peer Proxy is changed. The states 'active' and 'standby' are normal states.		
Raising condition: (('Local State' NOT EQUAL 'active') OR ('Local State' NOT EQUAL 'standby'))		
Clearing condition: (('Local State' EQUAL 'active') OR ('Local State' EQUAL 'standby'))		
Remedial action: Ensure Proxy multi-chassis redundancy is functionally up.		

Table 14-327 PTPClockNoMasterAlarm

Alarm	Attributes	Applicable major release
Name: PTPClockNoMasterAlarm (3604) Type: communicationsAlarm Package: ptp.PTPClockNoMasterAlarm Raised on class: ptp.IEEEPTPClock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPClockNoMaster	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Precision Timing Protocol (PTP) clock does not support PTP timing master.		
Remedial action: Informational- Please verify master clock configuration for timing.		

Table 14-328 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 14-329 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 14-330 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 14-331 PTPPortNoTimestamping

Alarm	Attributes	Applicable major release
Name: PTPPortNoTimestamping (8405) Type: communicationsAlarm Package: ptp.PTPPortNoTimestamping Raised on class: ptp.IEEEPTPPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PerformanceDegraded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The PtpPortNoTimestamping notification is generated when a PTP port is created and the associated Ethernet port does not support IEEE 1588-2008 port-based timestamping. The PTP port is created but the performance may be degraded due to timestamping at the CPM. For optimal performance, ensure PTP is enabled on ports with IEEE 1588-2008 port-based timestamping capability.		
Remedial action: The Ethernet port used for the PTP port should be changed to a port on an MDA that supports IEEE 1588-2008 port-based timestamping.		

Table 14-332 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 14-333 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 14-334 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-334 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 14-335 PXCAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: PXCAdministrativelyDown (11185) Type: equipmentAlarm Package: pxc.PXCAdministrativelyDown Raised on class: pxc.PortCrossConnect	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portCrossConnectAdministra-tivelyDown	Release: • 14.0
Description: The alarm is raised when the PXC AdministrativelyDown.		
Raising condition: ('Administrative State' EQUAL 'Down')		
Clearing condition: (('Administrative State' EQUAL 'Up'))		
Remedial action: Informational - PortCrossConnect AdministrativelyDown.		

Table 14-336 PXCDown

Alarm	Attributes	Applicable major release
Name: PXCDown (11186) Type: equipmentAlarm Package: pxc.PXCDown Raised on class: pxc.PortCrossConnect	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperablePortCrossConnect	Release: • 14.0
Description: The alarm is raised when the PXC is OperationallyDown.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: This alarm indicates an inoperable PortCrossConnect. Either the associated PhysicalPort or PortCrossConnectSub-ports are down.		

Table 14-337 RadiusAcctPlcyFailure

Alarm	Attributes	Applicable major release
Name: RadiusAcctPlcyFailure (363) Type: radiusAccountingPolicyAlarm Package: radiusaccounting.RadiusAcctPlcyFailure Raised on class: radiusaccounting.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: radiusAccountingRequestFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RADIUS accounting request is not successfully sent to any of the RADIUS servers specified in the RADIUS accounting policy.		
Remedial action: The Radius server(s) which are configured in the accounting policy are unreachable. This may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the Radius server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 14-338 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 14-339 radiusServerOutOfService (subscrauth)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: subscrauth.radiusServerOutOfService Raised on class: subscrauth.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: subAuthPlcyRadSerOperStatChg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-339 radiusServerOutOfService (subscrauth) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the subscriber authentication policy.		

Table 14-340 radiusServerOutOfService (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: radiusaccounting.radiusServerOutOfService Raised on class: radiusaccounting.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radAcctPlcyRadSerOper-StatChg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the RADIUS accounting policy.		

Table 14-341 radiusServerOverloaded (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOverloaded (3913) Type: communicationsAlarm Package: radiusaccounting.radiusServerOverloaded Raised on class: radiusaccounting.RadiusEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusServerRequestLimi-tReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RADIUS server is overloaded.		
Remedial action: Verify the RADIUS server is properly configured to process pending accounting requests at the desired rate and ensure that this rate matches the accounting request limit defined for this RADIUS server on the RADIUS accounting policy.		

Table 14-342 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 14-343 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 14-344 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 14-345 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 14-346 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 14-347 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 14-348 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-349 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 14-350 RPKISessionNotEstablished

Alarm	Attributes	Applicable major release
Name: RPKISessionNotEstablished (8136) Type: communicationsAlarm Package: rtr.RPKISessionNotEstablished Raised on class: rtr.RpkiSession	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RPKISessionNotEstablished	Release: • 12.0 • 13.0 • 14.0

Table 14-350 RPKISessionNotEstablished (continued)

Alarm	Attributes	Applicable major release
Description: The notification alarm is raised when the RPKI Session is not established.		
Raising condition: (('Session State' NOT EQUAL 'Established'))		
Clearing condition: (('Session State' EQUAL 'Established'))		
Remedial action: Make sure that the Cache server is reachable and is configured properly.		

Table 14-351 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 14-352 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 14-353 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 14-354 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 14-355 SapDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosDynamicExceeded (4890) Type: securityServiceOrMechanismViolation Package: service.SapDDosDynamicExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0

Table 14-355 SapDDosDynamicExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the protocol on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpDynamicExcd trap) and the alarm status is set as non-conformant When the SAP starts hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP completes hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 14-356 SapDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosLocMonitorExceeded (4891) Type: securityServiceOrMechanismViolation Package: service.SapDDosLocMonitorExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the SAP (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 14-357 SapDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosStaticExceeded (4892) Type: securityServiceOrMechanismViolation Package: service.SapDDosStaticExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0

Table 14-357 SapDDosStaticExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the static-policer on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpStaticExcd trap) and the alarm status is set as non-conformant. When the SAP starts hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP ends hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 14-358 SapSubAuthError

Alarm	Attributes	Applicable major release
Name: SapSubAuthError (8411) Type: processingErrorAlarm Package: service.SapSubAuthError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 14-359 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 14-360 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 14-361 scriptBackupLost

Alarm	Attributes	Applicable major release
Name: scriptBackupLost (273) Type: configurationAlarm Package: subscrident.scriptBackupLost Raised on class: subscrident.Policy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary subscriber identification script URL is operationally up, but a lower-priority script or URL is operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' EQUAL 'Up') AND (('Secondary Script Operational State' NOT EQUAL 'Up') OR ('Tertiary Script Operational State' NOT EQUAL 'Up')))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' NOT EQUAL 'Up') OR (('Secondary Script Operational State' EQUAL 'Up') AND ('Tertiary Script Operational State' EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 14-362 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 14-363 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 14-364 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 14-365 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 14-366 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-367 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 14-368 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 14-369 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-370 ServerDeclineStaticAddr

Alarm	Attributes	Applicable major release
Name: ServerDeclineStaticAddr (3951) Type: configurationAlarm Package: dhcp.ServerDeclineStaticAddr Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpClientHasStaticIpAddress	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The tmnxDhcpSvrDeclineStaticAddr notification is generated when a DHCP decline message is received from a DHCP client that has a static IP address assigned.		
Remedial action: DHCP client has a static IP address. Make sure that the DHCP client has a dynamic IP address		

Table 14-371 ServerLeaseDefaultTimers

Alarm	Attributes	Applicable major release
Name: ServerLeaseDefaultTimers (2937) Type: configurationAlarm Package: dhcp.ServerLeaseDefaultTimers Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: LeaseTimerInconsistent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the system has reverted to default lease timer values for a particular DHCP client because the configuration of the lease timers was inconsistent.		
Remedial action: This warning is generated when configuration of the lease timers of a particular DHCP client is inconsistent; the system has reverted to default lease timer values. \n The lease renew time T1 and lease rebind time T2 have been reverted to the default value of 1/2 and 2/3 of the lease time.\nPlease check the lease timers configuration on the local DHCP server to ensure the timers are compatible.		

Table 14-372 ServerMaxLeasesReached

Alarm	Attributes	Applicable major release
Name: ServerMaxLeasesReached (3316) Type: configurationAlarm Package: netw.ServerMaxLeasesReached Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMaxLeasesReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the maximum number of leases allocated by local DHCP server is reached.		

Table 14-372 ServerMaxLeasesReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - this alarm indicates that the maximum number of leases allocated by a local DHCP server was reached. The address ranges for existing address pools should be extended or a new address pool should be configured for the local DHCP server.		

Table 14-373 ServerMsgTooLong

Alarm	Attributes	Applicable major release
Name: ServerMsgTooLong (2938) Type: configurationAlarm Package: dhcp.ServerMsgTooLong Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMsgTooLong	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a DHCP message is generated but the message size exceeds either the maximum DHCP message size, or the size provided by the client in the option maximum DHCP message size.		
Remedial action: Review the access network DHCP configuration to ensure all parties send DHCP packets with appropriate message size.		

Table 14-374 ServerUserDatabaseUnknown

Alarm	Attributes	Applicable major release
Name: ServerUserDatabaseUnknown (3952) Type: configurationAlarm Package: dhcp.ServerUserDatabaseUnknown Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CannotFindUserDatabase	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The tmnxDhcpSvrUserDbUnknown notification is generated when the local DHCP server instance drops a DHCP message because a local user database with the name specified for this server instance could not be found.		
Remedial action: Please specify a valid local user database for this server instance.		

Table 14-375 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 14-376 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 14-377 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-378 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 14-379 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-380 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-381 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment. SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-382 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-383 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment.SonetPathPayloadMismatch Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 14-384 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 14-385 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment. SonetPathRemoteDefectIndication Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-386 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment. SonetPathUnequippedPathError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-387 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 14-388 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 14-389 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-389 SpbSiteDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 14-390 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 14-391 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 14-392 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 14-393 subHostInconsistentAtmTdOvr

Alarm	Attributes	Applicable major release
Name: subHostInconsistentAtmTdOvr (3685) Type: configurationAlarm Package: ressubscr.subHostInconsistentAtmTdOvr Raised on class: ressubscr.ResidentialSubscriberInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostInconsistentAtmTdOvr	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an AAA server (e.g. a RADIUS server) specifies an ATM Traffic Descriptor override for a subscriber host while it has already specified another one for another host on the same ATM Virtual Circuit.		
Remedial action: Modify the AAA configuration so that all subscriber hosts sharing the same ATM Virtual circuit use the same ATM Traffic Descriptor Override VSA. If different overrides are required, then the subscribers must be in different ATM Virtual Circuits.		

Table 14-394 SubHostLcktLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktLimitReached (4387) Type: configurationAlarm Package: netw.SubHostLcktLimitReached Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the system wide maximum number of lockout hosts is reached.		

Table 14-394 SubHostLcktLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout.		

Table 14-395 SubHostLcktSapLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktSapLimitReached (4391) Type: configurationAlarm Package: service.SubHostLcktSapLimitReached Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktSapLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the maximum number of lockout hosts on a given SAP is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout on the SAP.\n3. Change the Maximum Lockout Hosts (per SAP).		

Table 14-396 SubMcsRelatedProblem

Alarm	Attributes	Applicable major release
Name: SubMcsRelatedProblem (8404) Type: processingErrorAlarm Package: netw.SubMcsRelatedProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subMcsRelatedProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a subscriber management specific problem occurs during Multi Chassis Syncing, e.g. of DHCP lease states.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 14-397 SubnetDepleted

Alarm	Attributes	Applicable major release
Name: SubnetDepleted (3953) Type: configurationAlarm Package: dhcp.SubnetDepleted Raised on class: dhcp.Subnet	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Subnet becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a subnet becomes zero. Please create another subnet.		

Table 14-398 SubnetMinFreeExc

Alarm	Attributes	Applicable major release
Name: SubnetMinFreeExc (516) Type: configurationAlarm Package: dhcp.SubnetMinFreeExc Raised on class: dhcp.Subnet	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowSubnet-Min	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the actual number of free addresses in a subnet falls below the desired minimum number specified in the subnet configuration		
Remedial action: Please ensure that an adequate free address threshold is configured or create a new subnet to meet the system requirements. \nThis warning is raised on IPv4 DHCP servers only.		

Table 14-399 SubRadSapCoAError

Alarm	Attributes	Applicable major release
Name: SubRadSapCoAError (8416) Type: processingErrorAlarm Package: service.SubRadSapCoAError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: changeOfAddressError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that system was unable to process a Change of Authorization (CoA) request from a Radius server.		
Remedial action: Please ensure that Accept CoA attribute is properly enabled on the subscriber authentication policy defined for the service. Ensure that the object targeted by the CoA request (a subscriber host for example) is present on the router.		

Table 14-400 SubscriberAuthError (vprn)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: vprn.SubscriberAuthError Raised on class: vprn.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 14-401 SubscriberAuthError (ies)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: ies.SubscriberAuthError Raised on class: ies.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 14-402 SubscriberInterfaceDown

Alarm	Attributes	Applicable major release
Name: SubscriberInterfaceDown (440) Type: SubscriberInterfaceAlarm Package: service.SubscriberInterfaceDown Raised on class: service.SubscriberInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a subscriber interface is operationally down. The alarm clears when the subscriber interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		

Table 14-402 SubscriberInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 14-403 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 14-404 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 14-405 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 14-406 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 14-407 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		

Table 14-407 TmnxEqPortEtherLoopDetected (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 14-408 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 14-409 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 14-410 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 14-411 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 14-411 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 14-412 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 14-413 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 14-414 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 14-415 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-415 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 14-416 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 14-417 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		

Table 14-417 TxSectionSynchronizationError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 14-418 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 14-419 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 14-420 UnrecommendedNAT64DestinationPrefix

Alarm	Attributes	Applicable major release
Name: UnrecommendedNAT64DestinationPrefix (8060) Type: configurationAlarm Package: nat. UnrecommendedNAT64DestinationPrefix Raised on class: nat.Nat64Config	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unrecommendedConfiguration	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the bits [64-71] of NAT64 destination prefix are non-zero for prefix length of 96.		
Raising condition: (('NAT Destination Prefix Length' EQUAL '96') AND ('NAT Destination Prefix' NOT EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Clearing condition: (('NAT Destination Prefix Length' NOT EQUAL '96') OR ('NAT Destination Prefix' EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Remedial action: When using a prefix length 96, set the bits [64-71] of NAT64 Destination Prefix as zero.		

Table 14-421 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 14-422 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 14-423 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 14-424 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 14-424 UplinkPartiallyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 14-425 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 14-426 VideoInterfaceDown

Alarm	Attributes	Applicable major release
Name: VideoInterfaceDown (794) Type: VideoInterfaceAlarm Package: service.VideoInterfaceDown Raised on class: service.VideoInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a video interface is operationally down. The alarm clears when the video interface is operationally up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 14-427 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-428 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 14-429 VRtrIfDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosDynamicExceeded (4887) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosDynamicExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the protocol on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpDynamicExcd trap) and the alarm status is set as non-conformant When the network interface starts hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface completes hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 14-430 VRtrIfDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosLocMonitorExceeded (4888) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosLocMonitorExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the network interface (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 14-431 VRtrIfDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosStaticExceeded (4889) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosStaticExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the static-policer on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpStaticExcd trap) and the alarm status is set as non-conformant. When the network interface starts hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface ends hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 14-432 WaveTrackerEncoderDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderDegrade (821) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerEncoderDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderDegrade	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade')))		
Remedial action: The OT or SVAC card has detected a DSP failure and this means that the wavelength tracker encode power control is compromised. If this occurs during steady state operation, there is a high probability that the services carried by this OT or SVAC are unaffected. To clear this alarm, replace the card. The card replacement procedure is service affecting and should be conducted during a maintenance window.		

Table 14-433 WaveTrackerEncoderFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderFailure (822) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerEncoderFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure')))		
Remedial action: A cold reset, reseat, or replacement of a card is service impacting if the card is currently carrying services. If there are services currently carried over the card, it may be best to wait for a maintenance window before resetting, replacing, or reseating the card.Confirm that replacement OT or SVAC card supports the same band as the alarmed OT or SVAC card and connect all fibers to the replacement OT or SVAC card.		

Table 14-434 WaveTrackerMissingPluggableVOA

Alarm	Attributes	Applicable major release
Name: WaveTrackerMissingPluggableVOA (4618) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerMissingPluggableVOA Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingPluggableVOA	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA')))		
Remedial action: Informational - no corrective action required.		

Table 14-435 WaveTrackerPowerControlDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlDegrade (823) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlDegrade	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade')))		
Remedial action: check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.		

Table 14-436 WaveTrackerPowerControlFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlFailure (824) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure')))		
Remedial action: Either alarmed card has detected equipment problem or there is misfibering problem such that a light-emitting fiber has been plugged into the Tx port of aWavelength Tracker encoder-equipped transponder card.If the card is a transponder card that is equipped with aWavelength Tracker encoder, check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.the card is an SVAC, or if there is no fibering problem on the transponder card.Disconnect all fibers on the alarmed card and Replace the card. connect all fibers to the replacement card		

Table 14-437 WaveTrackerPowerControlHighlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlHighlimit (825) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlHighlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlHighlimit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 14-438 WaveTrackerPowerControllowlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControllowlimit (826) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControllowlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControllowlimit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control low limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 14-439 WppHostAuthenticationFailed

Alarm	Attributes	Applicable major release
Name: WppHostAuthenticationFailed (3916) Type: processingErrorAlarm Package: wpp.WppHostAuthenticationFailed Raised on class: wpp.Portal	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: portalWppHostAuthentication-Failure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a WPP host cannot be authenticated.		
Remedial action: The recovery action will depend on the exact failure cause as given by the failureReason.		

Table 14-440 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 14-441 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		

Table 14-441 XplError (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

15 7701 CPAA

15.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 15-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 15-2 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 15-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 15-4 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 15-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		

Table 15-5 AreaTypeMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 15-6 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 15-7 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 15-8 BgpASAdminDomainNumberMismatch

Alarm	Attributes	Applicable major release
Name: BgpASAdminDomainNumberMismatch (427) Type: configurationAlarm Package: topology. BgpASAdminDomainNumberMismatch Raised on class: topology.Cpaa	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configuredASNotMatchBg-pASAdminDomain	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a 7701 CPAA BGP AS does not match the BGP AS administrative domain.		
Raising condition: ('BGP AS Number Mismatch' EQUAL 'true')		
Clearing condition: ('BGP AS Number Mismatch' EQUAL 'false')		
Remedial action: The configured AS number for BGP AS and Sub-AS should match the configured values on the CPAA.		

Table 15-9 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-10 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 15-10 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 15-11 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 15-12 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 15-13 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 15-14 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 15-15 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 15-15 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 15-16 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 15-17 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 15-18 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0 • 7.0 • 8.0

Table 15-18 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 15-19 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 15-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 15-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 15-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 15-23 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		

Table 15-23 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-24 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 15-25 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 15-26 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 15-27 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 15-28 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		

Table 15-28 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 15-29 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 15-30 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 15-31 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 15-32 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 15-33 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.0 • 7.0 • 8.0

Table 15-33 EthernetPortNoFrameLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 15-34 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 15-35 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 15-36 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 15-37 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 15-38 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 15-39 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 15-40 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 15-41 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		

Table 15-41 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 15-42 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 15-43 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 15-44 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 15-45 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 15-46 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 15-47 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 15-48 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 15-49 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 15-49 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 15-50 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 15-51 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 15-52 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 15-53 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.0 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 15-54 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 15-55 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 15-56 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 15-56 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 15-57 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 15-58 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 15-59 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface is operationally down.		

Table 15-59 OspfInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 15-60 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 15-61 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 15-62 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 15-63 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 15-64 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 15-64 PeerDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-65 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-66 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 15-67 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 15-68 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 15-69 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.0 • 7.0 • 8.0

Table 15-69 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 15-70 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-71 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-72 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-73 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.0 • 7.0 • 8.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-74 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		

Table 15-74 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 15-75 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.0 • 7.0 • 8.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-76 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-77 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 15-78 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 15-79 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		

Table 15-79 PrimaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 15-80 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 15-81 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 15-82 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 15-83 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 15-84 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 15-85 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 15-86 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 15-87 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 15-87 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 15-88 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 15-89 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 15-90 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 15-91 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 15-92 TooManyCpaaForIsisLevel2

Alarm	Attributes	Applicable major release
Name: TooManyCpaaForIsisLevel2 (384) Type: configurationAlarm Package: topology.TooManyCpaaForIsisLevel2 Raised on class: topology.Cpaa	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyCpaaForIsisLevel2	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when there are too many 7701 CPAAs for IS-IS level 2.		
Raising condition: ('Too Many CPAAs (ISIS Level 2)' EQUAL 'true')		
Clearing condition: ('Too Many CPAAs (ISIS Level 2)' EQUAL 'false')		

Table 15-92 TooManyCpaaForIsisLevel2 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the configuration of CPAA and make sure there is at most one CPAA configured for ISIS level 2 within an administrative domain.		

Table 15-93 TooManyCpaaPerOspfArea

Alarm	Attributes	Applicable major release
Name: TooManyCpaaPerOspfArea (383) Type: configurationAlarm Package: topology.TooManyCpaaPerOspfArea Raised on class: topology.Cpaa	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyCpaaPerOspfArea	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when there are too many 7701 CPAAs for an OSPF area.		
Raising condition: ('Too Many CPAAs (OSPF Area)' EQUAL 'true')		
Clearing condition: ('Too Many CPAAs (OSPF Area)' EQUAL 'false')		
Remedial action: Check the configuration of CPAA and make sure there is at most one CPAA configured for an OSPF area within an administrative domain.		

Table 15-94 TooManyCpaaPerOspfv3Area

Alarm	Attributes	Applicable major release
Name: TooManyCpaaPerOspfv3Area (4397) Type: configurationAlarm Package: topology.TooManyCpaaPerOspfv3Area Raised on class: topology.Cpaa	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyCpaaPerOspfv3Area	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when there are too many 7701 CPAAs for an OSPF area.		
Raising condition: ('Too Many CPAAs (OSPFv3 Area)' EQUAL 'true')		
Clearing condition: ('Too Many CPAAs (OSPFv3 Area)' EQUAL 'false')		
Remedial action: Check the configuration of CPAA and make sure there is at most one CPAA configured for an OSPFv3 area within an administrative domain.		

Table 15-95 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 15-96 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.0 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		

Table 15-96 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 15-97 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.0 • 7.0 • 8.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 15-98 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 15-99 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 15-100 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 15-101 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 15-102 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 15-103 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 15-104 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 15-105 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 15-106 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

16 7705 SAR

16.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 16-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 16-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 16-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 16-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 16-5 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 16-6 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 16-7 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 16-8 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 16-9 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 16-10 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 16-11 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 16-12 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 16-13 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 16-14 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 16-15 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 16-16 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-17 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 16-18 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 16-19 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 16-20 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 16-21 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 16-22 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 16-23 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 16-24 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 16-25 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 16-26 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 16-27 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 16-28 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 16-29 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-30 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-31 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-32 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-33 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-34 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-35 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-36 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 16-37 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 16-38 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 16-39 ConcurrentSessionExceedsHigh

Alarm	Attributes	Applicable major release
Name: ConcurrentSessionExceedsHigh (5401) Type: thresholdCrossed Package: netw.ConcurrentSessionExceedsHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.1
Description: This alarm is raised when the concurrent security session count exceeds its high watermark. Cleared when it reaches its low watermark again; the watermarks are derived from the limit specified in hi-water-mark and low-water-mark.		
Remedial action: This alarm is raised when the concurrent security session count exceeds its high watermark.Cleared when it reaches its low watermark again; the watermarks are derived from the limit specified in hi-water-mark and low-water-mark.		

Table 16-40 ConcurrentSessionExhausted

Alarm	Attributes	Applicable major release
Name: ConcurrentSessionExhausted (5402) Type: thresholdCrossed Package: netw.ConcurrentSessionExhausted Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.1
Description: This alarm is raised when the concurrent security session count reaches the system limit. The concurrent session limit can be read in 'Concurrent Active Session Limit'.		
Remedial action: This alarm is raised when the concurrent security session count reaches the system limit.The concurrent session limit can be read in 'Concurrent Active Session Limit'		

Table 16-41 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 16-42 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 16-43 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 16-44 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 16-45 DataChannelAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DataChannelAlarmIndicationSignal (3944) Type: communicationsAlarm Package: tdmequipment. DataChannelAlarmIndicationSignal Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a data channel has an AIS alarm condition.		
Raising condition: (('Report Alarm Status'anyBit'Alarm Indication Signal') AND ('Report Alarm'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Alarm Indication Signal') AND ('Report Alarm'anyBit'Alarm Indication Signal')))		
Remedial action: The Cpipe Service running on this CODIR VT card need fixing. Make the Cpipe error free.		

Table 16-46 DataChannelLossOfSignal

Alarm	Attributes	Applicable major release
Name: DataChannelLossOfSignal (3946) Type: communicationsAlarm Package: tdmequipment.DataChannelLossOfSignal Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a date channel has an LOS condition.		
Raising condition: (('Report Alarm Status'anyBit'Loss Of Signal') AND ('Report Alarm'anyBit'Loss Of Signal'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Loss Of Signal') AND ('Report Alarm'anyBit'Loss Of Signal')))		
Remedial action: The Cpipe Service running on this VT card need fixing. Make the Cpipe error free.		

Table 16-47 DataChannelRemoteAlarmIndication

Alarm	Attributes	Applicable major release
Name: DataChannelRemoteAlarmIndication (3947) Type: communicationsAlarm Package: tdmequipment. DataChannelRemoteAlarmIndication Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmIndication	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a date channel has an RAI condition.		
Raising condition: (('Report Alarm Status'anyBit'Remote Alarm Indication') AND ('Report Alarm'anyBit'Remote Alarm Indication'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Alarm Indication') AND ('Report Alarm'anyBit'Remote Alarm Indication')))		
Remedial action: The Cpipe Service running on this TPIF VT card need fixing. Make the Cpipe error free.		

Table 16-48 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 16-49 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 16-50 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 16-51 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 16-52 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 16-53 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 16-54 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 16-55 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 16-56 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 16-57 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 16-58 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 16-59 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 16-60 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 16-61 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 16-62 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 16-63 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 16-64 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 16-65 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-66 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 16-67 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 16-68 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 16-69 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 16-70 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 16-71 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 16-72 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 16-73 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 16-74 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 16-75 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 16-76 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 16-77 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 16-78 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 16-79 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 16-80 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 16-81 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 16-82 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 16-83 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 16-84 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 16-85 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 16-86 GroupEncryptLabelConfigMismatch

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelConfigMismatch (8980) Type: configurationAlarm Package: nge.GroupEncryptLabelConfigMismatch Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label configuration mismatch is detected.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 16-87 GroupEncryptLabelCreationFailed

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelCreationFailed (8981) Type: communicationsAlarm Package: nge.GroupEncryptLabelCreationFailed Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label distribution fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		

Table 16-87 GroupEncryptLabelCreationFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 16-88 GroupEncryptLabelDeletionFailed

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelDeletionFailed (8982) Type: communicationsAlarm Package: nge.GroupEncryptLabelDeletionFailed Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label deletion fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 16-89 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 16-90 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 16-91 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 16-92 IncorrectNeighborConfig

Alarm	Attributes	Applicable major release
Name: IncorrectNeighborConfig (609) Type: configurationAlarm Package: aps.IncorrectNeighborConfig Raised on class: aps.ApsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incorrectNeighborConfig	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.		
Raising condition: (('Type' EQUAL 'MultiChassis') AND ('Neighbor match' EQUAL 'false'))		
Clearing condition: (('Type' EQUAL 'SingleChassis') OR ('Neighbor match' EQUAL 'true'))		
Remedial action: Make sure a peer exist and the neighbor address points to a network interface on the NE that contains the peer object.		

Table 16-93 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 16-94 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 16-95 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 16-96 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 4.0 • 5.0 • 6.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-97 IOMEventOverflow

Alarm	Attributes	Applicable major release
Name: IOMEventOverflow (5617) Type: equipmentAlarm Package: equipment.IOMEventOverflow Raised on class: equipment.BaseCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMEventOverflow	Release: • 7.0 • 8.0
Description: The alarm is generated when tmnxIomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimitReached occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.		
Remedial action: Informational - The alarm will be cleared when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.		

Table 16-98 IOMResUtilizationLimit

Alarm	Attributes	Applicable major release
Name: IOMResUtilizationLimit (5618) Type: equipmentAlarm Package: equipment.IOMResUtilizationLimit Raised on class: equipment.BaseCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMResHighLimitReached Applicable probable causes: • IOMResHighLimitReached • IOMResExhausted	Release: • 7.0 • 8.0
Description: The alarm is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the value of tmnxIomResourceLimitPct.		
Remedial action: Informational - The alarm will be cleared when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.		

Table 16-99 IPSecIsaGrpDown

Alarm	Attributes	Applicable major release
Name: IPSecIsaGrpDown (3745) Type: equipmentAlarm Package: isa.IPSecIsaGrpDown Raised on class: isa.IPSecIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPSecIsaGrpDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an ISA IPSec group is Down and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Tunnel Group is down, despite the administrative state being up. Check that the configured ISA-Tunnel Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application IPSec(Tunnel) Group.		

Table 16-100 IPSecTunnelBfdConnectionBroken

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionBroken Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 16-101 IPSecTunnelBfdConnectionDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 16-102 IPSecTunnelBfdConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm Package: ipsec. IPSecTunnelBfdConnectionPeerDetectsDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 16-103 IPSecTunnelDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelDown (834) Type: serviceAlarm Package: ipsec.IPSecTunnelDown Raised on class: ipsec.IPSecTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-103 IPSecTunnelDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the IPsec tunnel operational state changes to 'down' and the administrative state is 'up'.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 16-104 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 16-105 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 16-105 IsisDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 16-106 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 16-107 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		

Table 16-107 KeepAliveProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 16-108 KeyGroupActiveOutboundSAConfigPending

Alarm	Attributes	Applicable major release
Name: KeyGroupActiveOutboundSAConfigPending (8983) Type: configurationAlarm Package: nge.KeyGroupActiveOutboundSAConfigPending Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyGroupActiveOutboundSA-ConfigPending	Release: • 7.0 • 8.0
Description: The alarm is raised when the activeOutboundSA configuration stage fails during the encryption process. This alarm is cleared once the encryption process is successful.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Deployed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND (('Deployment Status' EQUAL 'Deployed and Egress-Active') OR ('Deployment Status' EQUAL 'Configuration Mismatch')))		
Remedial action: Active Outbound SA configuration of the keygroup is pending or failed. If the operation has failed retry encryption after isolating the problem.		

Table 16-109 KeyGroupConfigMismatch

Alarm	Attributes	Applicable major release
Name: KeyGroupConfigMismatch (8984) Type: configurationAlarm Package: nge.KeyGroupConfigMismatch Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group configuration mismatch is detected.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 16-110 KeyGroupCreationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupCreationFailed (8985) Type: communicationsAlarm Package: nge.KeyGroupCreationFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group distribution fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 16-111 KeyGroupDeletionFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupDeletionFailed (8986) Type: communicationsAlarm Package: nge.KeyGroupDeletionFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group deletion fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 16-112 KeyGroupEgressActivationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupEgressActivationFailed (8987) Type: configurationAlarm Package: nge.KeyGroupEgressActivationFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyActivationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when activation fails during key distribution.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Egress Activation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Egress Activation Failed'))		
Remedial action: Active Outbound SA configuration has failed. Please check for specific alarms and take appropriate action.		

Table 16-113 KeyGroupKeysConfigMismatch

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysConfigMismatch (8988) Type: configurationAlarm Package: nge.KeyGroupKeysConfigMismatch Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys configuration mismatch is detected.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 16-114 KeyGroupKeysCreationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysCreationFailed (8989) Type: communicationsAlarm Package: nge.KeyGroupKeysCreationFailed Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys distribution fails for a site.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 16-115 KeyGroupKeysDeletionFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysDeletionFailed (8990) Type: communicationsAlarm Package: nge.KeyGroupKeysDeletionFailed Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys deletion fails for a site.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 16-116 KeyGroupKeysVerificationPending

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysVerificationPending (8991) Type: configurationAlarm Package: nge.KeyGroupKeysVerificationPending Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VerificationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys verification is pending or failed. This alarm is cleared once the encryption process is successful.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Deployed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND (('Deployment Status' EQUAL 'Deployed and Verified') OR ('Deployment Status' EQUAL 'Configuration Mismatch')))		
Remedial action: Verification of security key deployed on the node is pending or it has failed. If the operation has failed retry encryption after isolating the problem. Delete the key from node CLI if problem persists.		

Table 16-117 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 16-118 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 16-119 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 16-120 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 16-121 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 16-122 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 16-123 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 16-124 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 16-125 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-126 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 16-127 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 16-128 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 16-129 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 16-130 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 16-131 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 16-132 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 16-133 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 16-134 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 16-135 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 16-136 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 16-137 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 16-138 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 16-139 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 16-140 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 16-141 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 16-142 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 16-143 MptSwReconcileFailure

Alarm	Attributes	Applicable major release
Name: MptSwReconcileFailure (11483) Type: equipmentAlarm Package: netw.MptSwReconcileFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SwReconcileFail	Release: • 8.0
Description: This alarm is generated when microwave MPT sw reconcile fails.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 16-144 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 16-145 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-146 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 16-147 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		

Table 16-147 NewSsh2ServerKeyDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 16-148 NGEUnsupportedVPRNSiteDetected

Alarm	Attributes	Applicable major release
Name: NGEUnsupportedVPRNSiteDetected (9011) Type: configurationAlarm Package: vprn.NGEUnsupportedVPRNSiteDetected Raised on class: vprn.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NGEUnsupported	Release: • 7.0 • 8.0
Description: The alarm is raised when the VPRN site does not support Network Group Encryption, and auto bind LDP option is enabled.		
Remedial action: The site which does not support Network Group Encryption and has auto bind LDP enabled is added to the VPRN service, remove this site from this VPRN.		

Table 16-149 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 16-150 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 16-151 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 4.0 • 5.0 • 6.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 16-152 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-152 NodeSuspended (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 16-153 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 16-154 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		

Table 16-154 OspfInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-155 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 16-156 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-156 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 16-157 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 16-158 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-158 PeerConnectionDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 16-159 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-160 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-160 PeerGroupDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-161 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 16-162 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-162 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 16-163 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 16-164 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		

Table 16-164 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 16-165 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 16-166 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 16-166 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 16-167 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-168 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when a DC failure occurs on the power supply.		

Table 16-168 PowerSupplyDcFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-169 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-170 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		

Table 16-170 PowerSupplyInputFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-171 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 16-172 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		

Table 16-172 PowerSupplyOutputFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-173 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-174 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 16-175 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 16-176 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 16-177 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 16-178 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 16-179 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 16-180 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 16-181 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 16-182 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 16-183 RadioNoDbFile

Alarm	Attributes	Applicable major release
Name: RadioNoDbFile (4905) Type: communicationsAlarm Package: mwa.RadioNoDbFile Raised on class: mwa.PortTermination	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoDbFile	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when SAR is not able detect the radio database file specified.		
Raising condition: ('Oper Flag'anyBit'No Database File')		
Clearing condition: NOT (('Oper Flag'anyBit'No Database File'))		
Remedial action: Please place a valid MPT radio database file in the SAR compact flash or do /admin save/ for the file to be created.		

Table 16-184 RadioNotPresent

Alarm	Attributes	Applicable major release
Name: RadioNotPresent (4845) Type: equipmentAlarm Package: mwa.RadioNotPresent Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RadioNotDetected	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a microwave radio device is no longer detected.		
Raising condition: ('Oper Flag'anyBit'Radio Not Present')		
Clearing condition: NOT (('Oper Flag'anyBit'Radio Not Present'))		
Remedial action: This notifications reports the management session to the MPR-e has been lost and the MPR-e is no longer reachable. Likely the MPR-e is resetting or has not yet connected to 7705 after a 7705 system or MDA reset.		

Table 16-185 RadioSoftwareDownloadFailed

Alarm	Attributes	Applicable major release
Name: RadioSoftwareDownloadFailed (4847) Type: communicationsAlarm Package: mwa.RadioSoftwareDownloadFailed Raised on class: mwa.RadioPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SoftwareDownloadFailure	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when software download fails		
Raising condition: ('Software State'anyBit'Download Failed')		
Clearing condition: NOT (('Software State'anyBit'Download Failed'))		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 16-186 RadioSoftwarePackageMissing

Alarm	Attributes	Applicable major release
Name: RadioSoftwarePackageMissing (4870) Type: NoValidRadioSoftwareFound Package: netw.RadioSoftwarePackageMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NoValidRadioSoftwareFound	Release: • 6.0
Description: This alarm is raised when SAR is missing a valid MPR-e SW package in SAR compact flash.		
Remedial action: This is raised when SAR is missing the MPR-e SW package in SAR compact Flash; remedial action is to download the SAR SW bundle including MPR-e package; likely someone removed explicitly MPR-e SW package folder or downloaded the wrong SAR SW bundle to the node		

Table 16-187 RadioTxMuted

Alarm	Attributes	Applicable major release
Name: RadioTxMuted (4849) Type: communicationsAlarm Package: mwa.RadioTxMuted Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RadioTransmitterMuted	Release: • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when microwave radio transmitter changes state.		
Raising condition: ('Oper Flag'anyBit'Tx Muted')		
Clearing condition: NOT (('Oper Flag'anyBit'Tx Muted'))		

Table 16-187 RadioTxMuted (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 16-188 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 16-189 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 16-189 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 16-190 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam.RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 16-191 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		

Table 16-191 RedundantMepMissing (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 16-192 RekeyCleanupFailed

Alarm	Attributes	Applicable major release
Name: RekeyCleanupFailed (9013) Type: configurationAlarm Package: nge.RekeyCleanupFailed Raised on class: nge.KeyGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RekeyCleanupFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Re-key fails during key cleanup.		
Raising condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' EQUAL 'Cleanup Failed')))		
Clearing condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' NOT EQUAL 'Cleanup Failed')))		
Remedial action: The Rekey cleanup process has failed. Please check for specific alarms on the Security Association objects and take appropriate action.		

Table 16-193 RekeyFailed

Alarm	Attributes	Applicable major release
Name: RekeyFailed (8993) Type: configurationAlarm Package: nge.RekeyFailed Raised on class: nge.KeyGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RekeyFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Re-key fails during key distribution or activation.		
Raising condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' EQUAL 'Key Deployment Failed') OR ('Rekey State' EQUAL 'Key Activation Failed')))		
Clearing condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' NOT EQUAL 'Key Deployment Failed') AND ('Rekey State' NOT EQUAL 'Key Activation Failed')))		
Remedial action: The Rekey process has failed. Please check for specific alarms on the Security Association objects and take appropriate action.		

Table 16-194 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 16-195 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 16-196 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-197 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 16-198 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 16-199 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 16-200 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 16-201 ScadaBranchSquelched

Alarm	Attributes	Applicable major release
Name: ScadaBranchSquelched (11240) Type: equipmentAlarm Package: equipment.ScadaBranchSquelched Raised on class: equipment.ScadaBranch	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SquelchStatusChanged	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This alarm is raised when a Scada branch is squelched.		
Remedial action: Perform a squelch reset at the bridge.		

Table 16-202 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 16-203 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 16-204 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 16-205 SDPDisableEncryptionFailed

Alarm	Attributes	Applicable major release
Name: SDPDisableEncryptionFailed (8994) Type: communicationsAlarm Package: nge.SDPDisableEncryptionFailed Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DisableEncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when disabling SDP encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 16-206 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 16-207 SDPEncryptionConfigMismatch

Alarm	Attributes	Applicable major release
Name: SDPEncryptionConfigMismatch (8995) Type: configurationAlarm Package: nge.SDPEncryptionConfigMismatch Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a SDP Key Group Id mismatch is detected on a site.		
Raising condition: (('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Modify the configuration from node CLI or retry encryption.		

Table 16-208 SDPEncryptionFailed

Alarm	Attributes	Applicable major release
Name: SDPEncryptionFailed (8996) Type: communicationsAlarm Package: nge.SDPEncryptionFailed Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when enabling SDP encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Creation Failed'))		

Table 16-208 SDPEncryptionFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node..		

Table 16-209 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 16-210 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		

Table 16-210 SectionB1Error (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-211 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 16-212 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		

Table 16-212 SectionLossOfSignal (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 16-213 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-214 SerialChannelOutOfFrame

Alarm	Attributes	Applicable major release
Name: SerialChannelOutOfFrame (808) Type: communicationsAlarm Package: tdmequipment.SerialChannelOutOfFrame Raised on class: tdmequipment.SerialChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a serial channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'HCM Out Of Frame') AND ('Report Alarms'anyBit'HCM Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'HCM Out Of Frame') AND ('Report Alarms'anyBit'HCM Out Of Frame')))		
Remedial action: The Cpipe Service running on this RS232 serial card need fixing. Make the Cpipe error free.		

Table 16-215 SerialChannelRemoteAlarmIndication

Alarm	Attributes	Applicable major release
Name: SerialChannelRemoteAlarmIndication (809) Type: communicationsAlarm Package: tdmequipment.SerialChannelRemoteAlarmIndication Raised on class: tdmequipment.SerialChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmIndication	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a serial channel has an RAI condition.		
Raising condition: (('Outstanding Alarms'anyBit'HCM Remote Alarm Indication') AND ('Report Alarms'anyBit'HCM Remote Alarm Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'HCM Remote Alarm Indication') AND ('Report Alarms'anyBit'HCM Remote Alarm Indication')))		
Remedial action: The Cpipe Service running on this RS232 serial card need fixing. Make the Cpipe error free.		

Table 16-216 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 16-217 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 16-218 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 4.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 16-219 SoftwareDownloadInProgress

Alarm	Attributes	Applicable major release
Name: SoftwareDownloadInProgress (4850) Type: communicationsAlarm Package: mwa.SoftwareDownloadInProgress Raised on class: mwa.RadioPortSpecifics	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RadioSoftwareDownloadIn-Progress	Release: • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when radio software download is in progress - Software download is requested or a forced download is triggered.		
Raising condition: ('Software State'anyBit'In Progress')		
Clearing condition: NOT (('Software State'anyBit'In Progress'))		
Remedial action: This is alarm for information only.Informational - no corrective action required.		

Table 16-220 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-221 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-222 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-223 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-224 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment.SonetPathPayloadMismatch Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 16-225 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 16-226 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteDefectIndication Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-227 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment. SonetPathUnequippedPathError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-228 StaticLabelMapValueInUse

Alarm	Attributes	Applicable major release
Name: StaticLabelMapValueInUse (8965) Type: configurationAlarm Package: mpls.StaticLabelMapValueInUse Raised on class: mpls.StaticLabelMap	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: StaticLabelMapInUseByNGE	Release: • 7.0 • 8.0
Description: The alarm is raised when a static LSP configured with a label-map value that is identical to Group Encryption Label, is detected.		
Remedial action: Change the Static Label-Map value such that it is different from Group Encryption Label.		

Table 16-229 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 16-230 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 16-231 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 16-232 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 16-233 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 16-234 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 16-235 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 16-236 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 16-237 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 16-238 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 16-239 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 16-240 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 16-241 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 16-242 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 16-243 TwampRefInactivityTimeout

Alarm	Attributes	Applicable major release
Name: TwampRefInactivityTimeout (4969) Type: communicationsAlarm Package: sas.TwampRefInactivityTimeout Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPReflectorInactivityTimeout	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: tmnxTwampSrvNotifClientAddrType, tmnxTwampSrvNotifClientAddr, aluTwampRefNotifLocalAddrType, aluTwampRefNotifLocalAddr, aluTwampRefNotifLocalPort, aluTwampRefNotifRemoteAddrType, aluTwampRefNotifRemoteAddr, aluTwampRefNotifRemotePort The alarm is raised when a TWAMP test session was disconnected by the TWAMP Reflector because the session was inactive for a period exceeding the reflector's inactivity timeout (Reflector Test Session Timeout). The TWAMP reflector cannot receive any traffic on the disconnected session. RECOVERY - Check the IP connectivity between this reflector and the TWAMP client.		
Remedial action: Verify the value of the ref-inactivity-timeout and modify it according to the operational needs.		

Table 16-244 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 16-245 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 16-246 UnknownGroupEncryptLabelDetected

Alarm	Attributes	Applicable major release
Name: UnknownGroupEncryptLabelDetected (8975) Type: configurationAlarm Package: netw.UnknownGroupEncryptLabelDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Group Encryption label is detected that was not created by NGE Manager.		
Remedial action: Delete the Security Label from node CLI which is not created using SAM Encryption Manager.		

Table 16-247 UnknownKeyGroupDetected

Alarm	Attributes	Applicable major release
Name: UnknownKeyGroupDetected (8976) Type: configurationAlarm Package: netw.UnknownKeyGroupDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group is detected that was not created by NGE Manager.		
Remedial action: Delete all the Keygroups from node CLI which are not created using SAM Encryption Manager.		

Table 16-248 UnknownKeyGroupKeysDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownKeyGroupKeysDetected (8977) Type: configurationAlarm Package: netw.UnknownKeyGroupKeysDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys are detected that were not created by NGE Manager.		
Remedial action: Delete all the Security Associations from node CLI which are not created using SAM Encryption Manager.		

Table 16-249 UnknownSDPKeyGroupIdDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownSDPKeyGroupIdDetected (8978) Type: configurationAlarm Package: netw.UnknownSDPKeyGroupIdDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an SDP which was not configured by NGE manager.		
Remedial action: Check for similar alarms on the Network Element or SDP Tunnel, and take the action specified.		

Table 16-250 UnknownVPRNKeyGroupIdDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownVPRNKeyGroupIdDetected (8979) Type: configurationAlarm Package: netw.UnknownVPRNKeyGroupIdDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an VPRN site which was not configured by NGE manager.		
Remedial action: Check for similar alarms on the Network Element or VPRN site, and take the action specified.		

Table 16-251 UnknownVPRNKeyGroupIdDetected (vprn)

Alarm	Attributes	Applicable major release
Name: UnknownVPRNKeyGroupIdDetected (8979) Type: configurationAlarm Package: vprn.UnknownVPRNKeyGroupIdDetected Raised on class: vprn.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an VPRN site which was not configured by NGE manager.		
Remedial action: Remove encryption for this VPRN from node CLI.		

Table 16-252 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 16-253 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 16-254 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 16-255 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 16-256 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 16-257 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 16-258 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-259 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 16-260 VPRNDisableEncryptionFailed

Alarm	Attributes	Applicable major release
Name: VPRNDisableEncryptionFailed (8998) Type: communicationsAlarm Package: nge.VPRNDisableEncryptionFailed Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DisableEncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when disabling VPRN encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node..		

Table 16-261 VPRNEncryptionConfigMismatch

Alarm	Attributes	Applicable major release
Name: VPRNEncryptionConfigMismatch (8999) Type: configurationAlarm Package: nge.VPRNEncryptionConfigMismatch Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a VPRN Key Group Id mismatch is detected on a site.		

Table 16-261 VPRNEncryptionConfigMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Modify the configuration from node CLI or retry encryption.		

Table 16-262 VPRNEncryptionFailed

Alarm	Attributes	Applicable major release
Name: VPRNEncryptionFailed (9000) Type: communicationsAlarm Package: nge.VPRNEncryptionFailed Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when enabling VPRN encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 16-263 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 16-264 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 4.0 • 5.0 • 6.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

17 7705 SAR-H

17.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 17-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 17-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 17-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 17-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 17-4 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 17-5 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 17-6 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 17-7 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 5.0 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 17-8 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 17-9 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-9 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 17-10 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 17-11 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		

Table 17-11 BerLineSignalFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 17-12 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 17-13 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 17-14 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 17-15 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		

Table 17-16 BITS2NotQualified (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 17-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 17-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 17-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 17-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 17-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-21 BITSReferenceLossOfSignal (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 17-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 17-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 17-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 17-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 17-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 17-27 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 17-28 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-29 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-30 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-31 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-32 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-33 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-34 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-35 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 17-36 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 17-37 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 17-38 ConcurrentSessionExceedsHigh

Alarm	Attributes	Applicable major release
Name: ConcurrentSessionExceedsHigh (5401) Type: thresholdCrossed Package: netw.ConcurrentSessionExceedsHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.1
Description: This alarm is raised when the concurrent security session count exceeds its high watermark. Cleared when it reaches its low watermark again; the watermarks are derived from the limit specified in hi-water-mark and low-water-mark.		

Table 17-38 ConcurrentSessionExceedsHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the concurrent security session count exceeds its high watermark.Cleared when it reaches its low watermark again; the watermarks are derived from the limit specified in hi-water-mark and low-water-mark.		

Table 17-39 ConcurrentSessionExhausted

Alarm	Attributes	Applicable major release
Name: ConcurrentSessionExhausted (5402) Type: thresholdCrossed Package: netw.ConcurrentSessionExhausted Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.1
Description: This alarm is raised when the concurrent security session count reaches the system limit. The concurrent session limit can be read in 'Concurrent Active Session Limit'.		
Remedial action: This alarm is raised when the concurrent security session count reaches the system limit.The concurrent session limit can be read in 'Concurrent Active Session Limit'		

Table 17-40 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 17-41 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 17-42 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 17-43 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 17-44 DataChannelAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DataChannelAlarmIndicationSignal (3944) Type: communicationsAlarm Package: tdmequipment.DataChannelAlarmIndicationSignal Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a data channel has an AIS alarm condition.		
Raising condition: (('Report Alarm Status'anyBit'Alarm Indication Signal') AND ('Report Alarm'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Alarm Indication Signal') AND ('Report Alarm'anyBit'Alarm Indication Signal')))		
Remedial action: The Cpipe Service running on this CODIR VT card need fixing. Make the Cpipe error free.		

Table 17-45 DataChannelLossOfSignal

Alarm	Attributes	Applicable major release
Name: DataChannelLossOfSignal (3946) Type: communicationsAlarm Package: tdmequipment.DataChannelLossOfSignal Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a date channel has an LOS condition.		
Raising condition: (('Report Alarm Status'anyBit'Loss Of Signal') AND ('Report Alarm'anyBit'Loss Of Signal'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Loss Of Signal') AND ('Report Alarm'anyBit'Loss Of Signal')))		
Remedial action: The Cpipe Service running on this VT card need fixing. Make the Cpipe error free.		

Table 17-46 DataChannelRemoteAlarmIndication

Alarm	Attributes	Applicable major release
Name: DataChannelRemoteAlarmIndication (3947) Type: communicationsAlarm Package: tdmequipment. DataChannelRemoteAlarmIndication Raised on class: tdmequipment.DataChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmIndication	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a date channel has an RAI condition.		
Raising condition: (('Report Alarm Status'anyBit'Remote Alarm Indication') AND ('Report Alarm'anyBit'Remote Alarm Indication'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Alarm Indication') AND ('Report Alarm'anyBit'Remote Alarm Indication')))		
Remedial action: The Cpipe Service running on this TPIF VT card need fixing. Make the Cpipe error free.		

Table 17-47 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-47 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 17-48 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 17-49 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 17-50 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 17-51 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 17-52 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-52 DS1E1ResourceAvailabilityIndicator (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 17-53 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 17-54 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 17-55 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 17-56 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 17-57 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 17-58 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 17-59 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-59 DS3E3ResourceAvailability (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 17-60 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 17-61 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		

Table 17-61 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 17-62 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 17-63 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-64 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 17-65 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 17-66 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-66 EquipmentRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 17-67 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 17-68 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		

Table 17-68 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 17-69 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 17-70 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 17-71 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 17-72 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 17-73 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 17-74 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 17-75 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 17-76 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 17-77 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 17-78 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 17-79 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 17-80 FWSessionExceededAlarm

Alarm	Attributes	Applicable major release
Name: FWSessionExceededAlarm (4619) Type: firewallAlarm Package: firewall.FWSessionExceededAlarm Raised on class: firewall.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FWMaxSessionExceeded	Release: • 5.0 • 6.1 • 6.2
Description: The alarm is raised when Max Sessions for firewall is exceeded.		
Raising condition: (('Total Sessions' EQUAL '10000'))		
Clearing condition: (('Total Sessions' NOT EQUAL '10000'))		
Remedial action: Please reduce the number of currently running sessions on Firewall.		

Table 17-81 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		

Table 17-81 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 17-82 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 17-83 GroupEncryptLabelConfigMismatch

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelConfigMismatch (8980) Type: configurationAlarm Package: nge.GroupEncryptLabelConfigMismatch Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label configuration mismatch is detected.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 17-84 GroupEncryptLabelCreationFailed

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelCreationFailed (8981) Type: communicationsAlarm Package: nge.GroupEncryptLabelCreationFailed Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label distribution fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 17-85 GroupEncryptLabelDeletionFailed

Alarm	Attributes	Applicable major release
Name: GroupEncryptLabelDeletionFailed (8982) Type: communicationsAlarm Package: nge.GroupEncryptLabelDeletionFailed Raised on class: nge.GroupEncryptionLabel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when the Group Encryption Label deletion fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 17-86 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 17-87 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 17-88 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 17-89 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-89 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 17-90 IPSecIsaGrpDown

Alarm	Attributes	Applicable major release
Name: IPSecIsaGrpDown (3745) Type: equipmentAlarm Package: isa.IPSecIsaGrpDown Raised on class: isa.IPSecIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPSecIsaGrpDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an ISA IPSec group is Down and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Tunnel Group is down, despite the administrative state being up. Check that the configured ISA-Tunnel Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application IPSec(Tunnel) Group.		

Table 17-91 IPSecTunnelBfdConnectionBroken

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionBroken Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 17-92 IPSecTunnelBfdConnectionDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 17-93 IPSecTunnelBfdConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm Package: ipsec. IPSecTunnelBfdConnectionPeerDetectsDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 17-94 IPSecTunnelDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelDown (834) Type: serviceAlarm Package: ipsec.IPSecTunnelDown Raised on class: ipsec.IPSecTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the IPsec tunnel operational state changes to 'down' and the administrative state is 'up'.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 17-94 IPSecTunnelDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Fix the errors indicated in operational flag.		

Table 17-95 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 17-96 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 17-97 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 17-98 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 17-99 KeyGroupActiveOutboundSAConfigPending

Alarm	Attributes	Applicable major release
Name: KeyGroupActiveOutboundSAConfigPending (8983) Type: configurationAlarm Package: nge.KeyGroupActiveOutboundSAConfigPending Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyGroupActiveOutboundSA-ConfigPending	Release: • 7.0 • 8.0

Table 17-99 KeyGroupActiveOutboundSAConfigPending (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the activeOutboundSA configuration stage fails during the encryption process. This alarm is cleared once the encryption process is successful.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Deployed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND (('Deployment Status' EQUAL 'Deployed and Egress-Active') OR ('Deployment Status' EQUAL 'Configuration Mismatch')))		
Remedial action: Active Outbound SA configuration of the keygroup is pending or failed. If the operation has failed retry encryption after isolating the problem.		

Table 17-100 KeyGroupConfigMismatch

Alarm	Attributes	Applicable major release
Name: KeyGroupConfigMismatch (8984) Type: configurationAlarm Package: nge.KeyGroupConfigMismatch Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group configuration mismatch is detected.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 17-101 KeyGroupCreationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupCreationFailed (8985) Type: communicationsAlarm Package: nge.KeyGroupCreationFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group distribution fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 17-102 KeyGroupDeletionFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupDeletionFailed (8986) Type: communicationsAlarm Package: nge.KeyGroupDeletionFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group deletion fails on a site.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 17-103 KeyGroupEgressActivationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupEgressActivationFailed (8987) Type: configurationAlarm Package: nge.KeyGroupEgressActivationFailed Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyActivationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when activation fails during key distribution.		
Raising condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Egress Activation Failed'))		
Clearing condition: (('Site ID' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Egress Activation Failed'))		
Remedial action: Active Outbound SA configuration has failed. Please check for specific alarms and take appropriate action.		

Table 17-104 KeyGroupKeysConfigMismatch

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysConfigMismatch (8988) Type: configurationAlarm Package: nge.KeyGroupKeysConfigMismatch Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys configuration mismatch is detected.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Delete the configuration from node CLI.		

Table 17-105 KeyGroupKeysCreationFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysCreationFailed (8989) Type: communicationsAlarm Package: nge.KeyGroupKeysCreationFailed Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CreationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys distribution fails for a site.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node, or configuration pre-exists on the node. For the second case remove the configuration from node CLI.		

Table 17-106 KeyGroupKeysDeletionFailed

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysDeletionFailed (8990) Type: communicationsAlarm Package: nge.KeyGroupKeysDeletionFailed Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeletionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys deletion fails for a site.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 17-107 KeyGroupKeysVerificationPending

Alarm	Attributes	Applicable major release
Name: KeyGroupKeysVerificationPending (8991) Type: configurationAlarm Package: nge.KeyGroupKeysVerificationPending Raised on class: nge.SecurityAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VerificationFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys verification is pending or failed. This alarm is cleared once the encryption process is successful.		
Raising condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND ('Deployment Status' EQUAL 'Deployed'))		
Clearing condition: (('siteId' NOT EQUAL '\"0.0.0.0\"') AND (('Deployment Status' EQUAL 'Deployed and Verified') OR ('Deployment Status' EQUAL 'Configuration Mismatch')))		
Remedial action: Verification of security key deployed on the node is pending or it has failed. If the operation has failed retry encryption after isolating the problem. Delete the key from node CLI if problem persists.		

Table 17-108 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 17-109 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 7.0 • 8.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 17-110 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 17-111 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 17-112 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-112 LdpSessionNonexistent (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 17-113 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 17-114 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 17-115 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 17-116 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-117 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 17-118 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 17-119 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 17-120 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 17-121 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 17-122 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 17-123 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 17-124 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 17-125 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-125 macMoveRateExceeded (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 17-126 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 17-127 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 17-128 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 17-129 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 17-130 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-130 MplsDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 17-131 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 17-132 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		

Table 17-132 MvrSiteDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 17-133 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 17-134 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		

Table 17-134 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 17-135 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 17-136 NGEUnsupportedVPRNSiteDetected

Alarm	Attributes	Applicable major release
Name: NGEUnsupportedVPRNSiteDetected (9011) Type: configurationAlarm Package: vprn.NGEUnsupportedVPRNSiteDetected Raised on class: vprn.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NGEUnsupported	Release: • 7.0 • 8.0
Description: The alarm is raised when the VPRN site does not support Network Group Encryption, and auto bind LDP option is enabled.		
Remedial action: The site which does not support Network Group Encryption and has auto bind LDP enabled is added to the VPRN service, remove this site from this VPRN.		

Table 17-137 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 17-138 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 17-139 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 17-140 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 17-141 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 17-142 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 17-143 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 17-144 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 17-145 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 17-146 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-147 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-148 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 17-149 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 17-150 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 17-151 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 17-152 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 17-153 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 17-154 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-155 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-156 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-157 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-158 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 17-159 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-160 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-161 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 17-162 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 17-163 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 17-164 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 17-165 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 17-166 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 17-167 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 17-168 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 17-169 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-169 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 17-170 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 17-171 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 17-171 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 17-172 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 17-173 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 17-174 RekeyCleanupFailed

Alarm	Attributes	Applicable major release
Name: RekeyCleanupFailed (9013) Type: configurationAlarm Package: nge.RekeyCleanupFailed Raised on class: nge.KeyGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RekeyCleanupFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Re-key fails during key cleanup.		
Raising condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' EQUAL 'Cleanup Failed')))		
Clearing condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' NOT EQUAL 'Cleanup Failed')))		
Remedial action: The Rekey cleanup process has failed. Please check for specific alarms on the Security Association objects and take appropriate action.		

Table 17-175 RekeyFailed

Alarm	Attributes	Applicable major release
Name: RekeyFailed (8993) Type: configurationAlarm Package: nge.RekeyFailed Raised on class: nge.KeyGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RekeyFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when Re-key fails during key distribution or activation.		
Raising condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' EQUAL 'Key Deployment Failed') OR ('Rekey State' EQUAL 'Key Activation Failed')))		
Clearing condition: (('Site ID' EQUAL '\"0.0.0.0\"') AND (('Rekey State' NOT EQUAL 'Key Deployment Failed') AND ('Rekey State' NOT EQUAL 'Key Activation Failed')))		
Remedial action: The Rekey process has failed. Please check for specific alarms on the Security Association objects and take appropriate action.		

Table 17-176 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		

Table 17-176 RemoteMepCCMAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 17-177 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 17-178 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 17-179 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 17-180 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 17-181 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-181 RxSectionSynchronizationError (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 17-182 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 17-183 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 17-183 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 17-184 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 17-185 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 17-186 SDPDisableEncryptionFailed

Alarm	Attributes	Applicable major release
Name: SDPDisableEncryptionFailed (8994) Type: communicationsAlarm Package: nge.SDPDisableEncryptionFailed Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DisableEncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when disabling SDP encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 17-187 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 17-188 SDPEncryptionConfigMismatch

Alarm	Attributes	Applicable major release
Name: SDPEncryptionConfigMismatch (8995) Type: configurationAlarm Package: nge.SDPEncryptionConfigMismatch Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a SDP Key Group Id mismatch is detected on a site.		
Raising condition: (('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Modify the configuration from node CLI or retry encryption.		

Table 17-189 SDPEncryptionFailed

Alarm	Attributes	Applicable major release
Name: SDPEncryptionFailed (8996) Type: communicationsAlarm Package: nge.SDPEncryptionFailed Raised on class: nge.KeyGroupSdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when enabling SDP encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node..		

Table 17-190 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 17-191 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-191 SectionB1Error (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-192 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 17-193 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		

Table 17-193 SectionLossOfSignal (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 17-194 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-195 SerialChannelOutOfFrame

Alarm	Attributes	Applicable major release
Name: SerialChannelOutOfFrame (808) Type: communicationsAlarm Package: tdmequipment.SerialChannelOutOfFrame Raised on class: tdmequipment.SerialChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a serial channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'HCM Out Of Frame') AND ('Report Alarms'anyBit'HCM Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'HCM Out Of Frame') AND ('Report Alarms'anyBit'HCM Out Of Frame')))		
Remedial action: The Cpipe Service running on this RS232 serial card need fixing. Make the Cpipe error free.		

Table 17-196 SerialChannelRemoteAlarmIndication

Alarm	Attributes	Applicable major release
Name: SerialChannelRemoteAlarmIndication (809) Type: communicationsAlarm Package: tdmequipment.SerialChannelRemoteAlarmIndication Raised on class: tdmequipment.SerialChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmIndication	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a serial channel has an RAI condition.		
Raising condition: (('Outstanding Alarms'anyBit'HCM Remote Alarm Indication') AND ('Report Alarms'anyBit'HCM Remote Alarm Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'HCM Remote Alarm Indication') AND ('Report Alarms'anyBit'HCM Remote Alarm Indication')))		
Remedial action: The Cpipe Service running on this RS232 serial card need fixing. Make the Cpipe error free.		

Table 17-197 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 17-198 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 17-199 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 17-200 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		

Table 17-200 SonetPathAlarmIndicationSignal (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-201 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-202 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		

Table 17-202 SonetPathLossOfCodegroupDelineationError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-203 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-204 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment.SonetPathPayloadMismatch Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 17-205 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 17-206 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteDefectIndication Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-207 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment.SonetPathUnequippedPathError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-208 StaticLabelMapValueInUse

Alarm	Attributes	Applicable major release
Name: StaticLabelMapValueInUse (8965) Type: configurationAlarm Package: mpls.StaticLabelMapValueInUse Raised on class: mpls.StaticLabelMap	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: StaticLabelMapInUseByNGE	Release: • 7.0 • 8.0
Description: The alarm is raised when a static LSP configured with a label-map value that is identical to Group Encryption Label, is detected.		
Remedial action: Change the Static Label-Map value such that it is different from Group Encryption Label.		

Table 17-209 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 17-209 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 17-210 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 17-211 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 17-212 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 17-213 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 17-214 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 17-215 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 17-216 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 17-217 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 17-217 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 17-218 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 17-219 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 17-220 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 17-221 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-221 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 17-222 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 17-223 TwampRefInactivityTimeout

Alarm	Attributes	Applicable major release
Name: TwampRefInactivityTimeout (4969) Type: communicationsAlarm Package: sas.TwampRefInactivityTimeout Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPReflectorInactivityTimeout	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: tmnxTwampSrvNotifClientAddrType, tmnxTwampSrvNotifClientAddr, aluTwampRefNotifLocalAddrType, aluTwampRefNotifLocalAddr, aluTwampRefNotifLocalPort, aluTwampRefNotifRemoteAddrType, aluTwampRefNotifRemoteAddr, aluTwampRefNotifRemotePort The alarm is raised when a TWAMP test session was disconnected by the TWAMP Reflector because the session was inactive for a period exceeding the reflector's inactivity timeout (Reflector Test Session Timeout). The TWAMP reflector cannot receive any traffic on the disconnected session. RECOVERY - Check the IP connectivity between this reflector and the TWAMP client.		
Remedial action: Verify the value of the ref-inactivity-timeout and modify it according to the operational needs.		

Table 17-224 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 17-225 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 17-226 UnknownGroupEncryptLabelDetected

Alarm	Attributes	Applicable major release
Name: UnknownGroupEncryptLabelDetected (8975) Type: configurationAlarm Package: netw.UnknownGroupEncryptLabelDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0

Table 17-226 UnknownGroupEncryptLabelDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a Group Encryption label is detected that was not created by NGE Manager.		
Remedial action: Delete the Security Label from node CLI which is not created using SAM Encryption Manager.		

Table 17-227 UnknownKeyGroupDetected

Alarm	Attributes	Applicable major release
Name: UnknownKeyGroupDetected (8976) Type: configurationAlarm Package: netw.UnknownKeyGroupDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group is detected that was not created by NGE Manager.		
Remedial action: Delete all the Keygroups from node CLI which are not created using SAM Encryption Manager.		

Table 17-228 UnknownKeyGroupKeysDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownKeyGroupKeysDetected (8977) Type: configurationAlarm Package: netw.UnknownKeyGroupKeysDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when Key Group Keys are detected that were not created by NGE Manager.		
Remedial action: Delete all the Security Associations from node CLI which are not created using SAM Encryption Manager.		

Table 17-229 UnknownSDPKeyGroupIdDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownSDPKeyGroupIdDetected (8978) Type: configurationAlarm Package: netw.UnknownSDPKeyGroupIdDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an SDP which was not configured by NGE manager.		
Remedial action: Check for similar alarms on the Network Element or SDP Tunnel, and take the action specified.		

Table 17-230 UnknownVPRNKeyGroupIdDetected (netw)

Alarm	Attributes	Applicable major release
Name: UnknownVPRNKeyGroupIdDetected (8979) Type: configurationAlarm Package: netw.UnknownVPRNKeyGroupIdDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an VPRN site which was not configured by NGE manager.		
Remedial action: Check for similar alarms on the Network Element or VPRN site, and take the action specified.		

Table 17-231 UnknownVPRNKeyGroupIdDetected (vprn)

Alarm	Attributes	Applicable major release
Name: UnknownVPRNKeyGroupIdDetected (8979) Type: configurationAlarm Package: vprn.UnknownVPRNKeyGroupIdDetected Raised on class: vprn.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • 7.0 • 8.0
Description: The alarm is raised when a Key Group Id is configured on an VPRN site which was not configured by NGE manager.		
Remedial action: Remove encryption for this VPRN from node CLI.		

Table 17-232 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 17-233 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 17-234 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 17-235 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 17-236 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 17-237 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0

Table 17-237 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 17-238 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 17-239 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		

Table 17-239 VirtualNeighborDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 17-240 VPRNDisableEncryptionFailed

Alarm	Attributes	Applicable major release
Name: VPRNDisableEncryptionFailed (8998) Type: communicationsAlarm Package: nge.VPRNDisableEncryptionFailed Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DisableEncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when disabling VPRN encryption fails on a site.		
Raising condition: (('ngeLastActionStatus' EQUAL 'Deletion Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Deletion Failed'))		
Remedial action: This could be due to communication failure with the node..		

Table 17-241 VPRNEncryptionConfigMismatch

Alarm	Attributes	Applicable major release
Name: VPRNEncryptionConfigMismatch (8999) Type: configurationAlarm Package: nge.VPRNEncryptionConfigMismatch Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.0 • 8.0
Description: The alarm is raised when a VPRN Key Group Id mismatch is detected on a site.		
Raising condition: (('Deployment Status' EQUAL 'Configuration Mismatch'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Configuration Mismatch'))		
Remedial action: Modify the configuration from node CLI or retry encryption.		

Table 17-242 VPRNEncryptionFailed

Alarm	Attributes	Applicable major release
Name: VPRNEncryptionFailed (9000) Type: communicationsAlarm Package: nge.VPRNEncryptionFailed Raised on class: nge.KeyGroupVrfBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncryptionFailed	Release: • 7.0 • 8.0
Description: The alarm is raised when enabling VPRN encryption fails on a site.		

Table 17-242 VPRNEncryptionFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('ngeLastActionStatus' EQUAL 'Creation Failed'))		
Clearing condition: (('ngeLastActionStatus' NOT EQUAL 'Creation Failed'))		
Remedial action: This could be due to communication failure with the node.		

Table 17-243 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 17-244 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 5.0 • 6.1 • 6.2 • 7.0 • 8.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

18 7710 SR

18.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 18-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 18-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 18-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 18-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 18-5 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		

Table 18-5 AncillaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 18-6 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 18-7 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 18-8 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 18-9 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 18-10 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		

Table 18-10 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 18-11 backupScriptInUse

Alarm	Attributes	Applicable major release
Name: backupScriptInUse (274) Type: configurationAlarm Package: subscrident.backupScriptInUse Raised on class: subscrident.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupInUse	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the primary subscriber identification script is operationally down, but one of the other scripts is operationally up.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND (('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR (('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 18-12 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 18-13 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 18-14 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 18-15 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		

Table 18-15 BfdInterfaceConnectionBroken (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 18-16 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 18-17 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 18-18 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-19 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 18-20 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 18-21 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 18-22 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 18-23 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 18-24 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 18-25 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 18-26 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 18-27 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 18-28 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 18-29 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 10.0 • 11.0 • 12.0

Table 18-29 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 18-30 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 18-31 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-32 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-33 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-34 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-35 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-36 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-37 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-38 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 18-39 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 18-40 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 18-41 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 18-42 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback. ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 18-43 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 18-44 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 18-45 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 18-46 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback. ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 18-47 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 18-48 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 18-49 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 18-50 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 18-51 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 18-52 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 18-52 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 18-53 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 18-54 DhcpLseStateMobilityError

Alarm	Attributes	Applicable major release
Name: DhcpLseStateMobilityError (8409) Type: configurationAlarm Package: service.DhcpLseStateMobilityError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapDHCPLseStateMobilityError	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates that the system was unable to perform a mobility check for this lease state.		
Remedial action: Please make sure that host-connectivity-verify is enabled on the SAP.		

Table 18-55 DhcpLseStateRestoreProblem

Alarm	Attributes	Applicable major release
Name: DhcpLseStateRestoreProblem (8402) Type: processingErrorAlarm Package: netw.DhcpLseStateRestoreProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpLseStateRestoreProblem	Release: • 10.0 • 11.0 • 12.0

Table 18-55 DhcpLseStateRestoreProblem (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when an error is detected while processing a persistency record.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 18-56 DhcpMiscellaneousProblem

Alarm	Attributes	Applicable major release
Name: DhcpMiscellaneousProblem (8403) Type: processingErrorAlarm Package: netw.DhcpMiscellaneousProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpMiscellaneousProblem	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a miscellaneous DHCP problem occurs.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 18-57 DHCPPoolFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPPoolFailoverStateChange (5168) Type: configurationAlarm Package: dhcp.DHCPPoolFailoverStateChange Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPPoolFailoverStat-eChanged	Release: • 11.0 • 12.0
Description: The alarm is raised when the Local DHCP Pool Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when the operational state of a particular Local DHCP Pool Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a pool failover is in progress.\nThis alarm is cleared implicitly when the DHCP Pool Failover state returns to Normal.		

Table 18-58 DHCPServerFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPServerFailoverStateChange (4986) Type: configurationAlarm Package: dhcp.DHCPServerFailoverStateChange Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPServerFailoverStateChanged	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Local DHCP Server Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when operational state of a particular Local DHCP Server Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a server failover is in progress.\nThis alarm will be cleared implicitly when the DHCP Server Failover state returns to Normal.		

Table 18-59 DHCPSFoLeaseUpdateFailedAddressConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedAddressConflict (4977) Type: configurationAlarm Package: dhcp.DHCPSFoLeaseUpdateFailedAddressConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFailedAddressConflict	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a address conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased another address to this host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased another address to this host. Please ensure all configuration is correct.		

Table 18-60 DHCPSFoLeaseUpdateFailedfoShutdown

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedfoShutdown (4985) Type: configurationAlarm Package: dhcp.DHCPSFoLeaseUpdateFailedfoShutdown Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFailedfoShutdown	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a shutdown lease update received from the failover peer cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'.		

Table 18-60 DHCPSFoLeaseUpdateFailedfoShutdown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'. Please ensure all configuration is correct.		

Table 18-61 DHCPSFoLeaseUpdateFailedHostConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedHostConflict (4978) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedHostConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedHostConflict	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a host conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased this address to another host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased this address to another host. Please ensure all configuration is correct.		

Table 18-62 DHCPSFoLeaseUpdateFailedLeaseExpired

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedLeaseExpired (4979) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedLeaseExpired Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedLeaseExpired	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a lease expired lease update received from the failover peer cannot be processed successfully. The lease received from the peer has expired.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer has expired. Please ensure all configuration is correct.		

Table 18-63 DHCPSFoLeaseUpdateFailedMaxLeaseReached

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedMax-LeaseReached (4980) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedMaxLeaseReached Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedMaxLeaseReached	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a maximum reached lease update received from the failover peer cannot be processed successfully. The maximum number of leases is already reached.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The maximum number of leases is already reached. Please ensure all configuration is correct.		

Table 18-64 DHCPSFoLeaseUpdateFailedPeerConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPeerConflict (4981) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPeerConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPeerConflict	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a peer conflict lease update received from the failover peer cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance. Please ensure all configuration is correct.		

Table 18-65 DHCPSFoLeaseUpdateFailedPersistenceCongested

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPer-sistenceCongested (4982) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPersistenceCongested Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPersistenceCongested	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a persistence congested lease update received from the failover peer cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload. Please ensure all configuration is correct.		

Table 18-66 DHCPSFoLeaseUpdateFailedRangeNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedRangeNotFound (4983) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedRangeNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFaile-dRangeNotFound	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a range not found lease update received from the failover peer cannot be processed successfully. No valid include range for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid include range for this lease could be found. Please ensure all configuration is correct.		

Table 18-67 DHCPSFoLeaseUpdateFailedSubnetNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedSubnetNotFound (4984) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedSubnetNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedSubnetNotFound	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a subnet not found lease update received from the failover peer cannot be processed successfully. No valid subnet for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid subnet for this lease could be found. Please ensure all configuration is correct.		

Table 18-68 DhcpSvrNoSubnetFixAddr

Alarm	Attributes	Applicable major release
Name: DhcpSvrNoSubnetFixAddr (8378) Type: configurationAlarm Package: dhcp.DhcpSvrNoSubnetFixAddr Raised on class: dhcp.LocalDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpSvrNoSubnetFixAddr	Release: • 10.0 • 11.0 • 12.0
Description: This alarm can be generated for hosts configured with a fixed IP address in the local user database. If such a host requests an ip-address and the system cannot find a matching subnet in this server instance for this IP address, then this alarm is generated, and the request is dropped.		
Remedial action: Ensure that the IP Address configured for this host under the local user database falls into a subnet under the local DHCP server mapped to this alarm.		

Table 18-69 DiamAppMessageDropped

Alarm	Attributes	Applicable major release
Name: DiamAppMessageDropped (5175) Type: processingErrorAlarm Package: diameter.DiamAppMessageDropped Raised on class: diameter.DiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamAppMessageDropped	Release: • 12.0
Description: The alarm is raised when the Diameter protocol has dropped a message		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 18-70 DiamAppSessionFailure

Alarm	Attributes	Applicable major release
Name: DiamAppSessionFailure (5410) Type: processingErrorAlarm Package: ressubscr.DiamAppSessionFailure Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamAppSessionFailure	Release: • 12.0
Description: The alarm is raised when the Diameter protocol has a session failure.		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 18-71 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 18-72 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 18-73 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 18-74 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 18-75 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 18-76 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment.DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 18-77 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		

Table 18-77 DS1E1SignalDegradation (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 18-78 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 18-79 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 18-80 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		

Table 18-80 DS3E3Looped (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 18-81 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 18-82 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 18-83 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 18-84 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 18-85 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		

Table 18-85 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 18-86 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 18-87 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 18-88 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-89 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 18-90 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		

Table 18-90 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 18-91 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 18-92 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 18-93 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 18-94 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 18-95 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		

Table 18-95 EthernetPortHighBer (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 18-96 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 18-97 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 18-98 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 18-99 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 18-100 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 10.0 • 11.0 • 12.0

Table 18-100 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 18-101 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 18-102 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 18-103 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 18-104 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 18-105 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		

Table 18-105 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational		

Table 18-106 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 18-107 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 18-108 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 18-109 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 18-110 GroupInterfaceDown

Alarm	Attributes	Applicable major release
Name: GroupInterfaceDown (441) Type: GroupInterfaceAlarm Package: service.GroupInterfaceDown Raised on class: service.GroupInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that a group interface is operationally down. The alarm clears when the group interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		

Table 18-110 GroupInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 18-111 HostConnectivityLostRateExceeded

Alarm	Attributes	Applicable major release
Name: HostConnectivityLostRateExceeded (276) Type: communicationsAlarm Package: ressubscr. HostConnectivityLostRateExceeded Raised on class: ressubscr.ShcvSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hostDown Applicable probable causes: • hostDown • trapDropped	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the trapDroppedRaisesAlarm parameter is enabled and the maximum allowed number of SHCV host connectivity loss events on a SAP is exceeded. The SHCV action in response to the alarm is specified by the maxHostLostConnectivityRate parameter. If the specified action is to remove the host information, the host information is removed and the connectivity of the host is not subsequently verified.		
Remedial action: This may be a transient error condition in the network or possible congestion or could be a sign that the SHCV ping interval is too short. Verify the status of the network for those subscribers and the service SHCV configuration.		

Table 18-112 IGHMisconfigured

Alarm	Attributes	Applicable major release
Name: IGHMisconfigured (827) Type: ighAlarm Package: igh.IGHMisconfigured Raised on class: igh.InterfaceGroupHandler	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IGHProtocolMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the IGH is administratively up but none of the IGH protocols is operationally up.		
Raising condition: (('igh_misconfigured' EQUAL '\"yes\"') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('igh_misconfigured' NOT EQUAL '\"yes\"') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Please check the configuration.		

Table 18-113 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 18-114 IgmpMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxGrpSrcsLimitExceeded (4624) Type: configurationAlarm Package: igmp.IgmpMaxGrpSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0
Description: The alarm is raised when an attempt is made to configure an IGMP group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Needs to increase 'maxGrpSources' value to allow more sources on this interface.		

Table 18-115 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 18-116 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 18-117 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 18-118 IncorrectNeighborConfig

Alarm	Attributes	Applicable major release
Name: IncorrectNeighborConfig (609) Type: configurationAlarm Package: aps.IncorrectNeighborConfig Raised on class: aps.ApsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incorrectNeighborConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.		
Raising condition: (('Type' EQUAL 'MultiChassis') AND ('Neighbor match' EQUAL 'false'))		
Clearing condition: (('Type' EQUAL 'SingleChassis') OR ('Neighbor match' EQUAL 'true'))		

Table 18-118 IncorrectNeighborConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: Make sure a peer exist and the neighbor address points to a network interface on the NE that contains the peer object.		

Table 18-119 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 18-120 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 18-121 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 18-122 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 18-123 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 18-124 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 18-125 InterfaceDown (service)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: service.InterfaceDown Raised on class: service.RedundantInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that a redundant interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 18-126 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		

Table 18-126 InterfaceDown (vpls) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 18-127 InterfaceDown (vprn)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vprn.InterfaceDown Raised on class: vprn.IPMirrorInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that an interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 18-128 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-129 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 18-130 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 18-131 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 18-132 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 18-133 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 18-134 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		

Table 18-134 LagDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 18-135 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 18-136 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 18-137 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 18-138 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 18-139 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 18-140 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 18-141 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-142 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		

Table 18-142 LineRemoteDefectIndication (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 18-143 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 18-144 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 18-145 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 18-146 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 18-147 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 18-147 LspDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 18-148 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 18-149 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 18-150 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0

Table 18-150 macMoveRateExceeded (service) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 18-151 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 18-152 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 18-153 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis.MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 18-154 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 18-155 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MC endpoint is operationally down.		

Table 18-155 MCPeerEPDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 18-156 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 18-157 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 18-158 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 18-159 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 18-160 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 18-161 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 18-162 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 18-163 MsdpDown

Alarm	Attributes	Applicable major release
Name: MsdpDown (353) Type: ProtocolAlarm Package: msdp.MsdpDown Raised on class: msdp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the MSDP site.		

Table 18-164 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 18-165 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 18-166 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNotExist	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 18-167 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNotExist	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 18-168 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		

Table 18-168 MvrSiteDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 18-169 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-170 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 10.0 • 11.0 • 12.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		

Table 18-170 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 18-171 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 18-172 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 18-173 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 18-174 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 18-175 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 18-176 noFunctioningScript

Alarm	Attributes	Applicable major release
Name: noFunctioningScript (275) Type: configurationAlarm Package: subscrident.noFunctioningScript Raised on class: subscrident.Policy	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryBackupDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all subscriber identification scripts are operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND ('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR ('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 18-177 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 18-178 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		

Table 18-178 NTPOperDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 18-179 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-180 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 18-181 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 18-182 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 18-183 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 10.0 • 11.0 • 12.0

Table 18-183 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 18-184 PeerConnectionDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: msdp.PeerConnectionDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.		
Raising condition: (('connectionState' NOT EQUAL 'Established') AND ('administrativeState' EQUAL 'Up'))		
Clearing condition: (('connectionState' EQUAL 'Established') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Check the configurations of the peer routers.		

Table 18-185 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 18-186 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-187 PeerDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: msdp.PeerDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('administrativeState' EQUAL 'Down'))		
Clearing condition: (('administrativeState' NOT EQUAL 'Down'))		
Remedial action: Turn up the Peer.		

Table 18-188 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 18-188 PeerGroupDown (bgp) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-189 PeerGroupDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: msdp.PeerGroupDown Raised on class: msdp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the Group.		

Table 18-190 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 18-191 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 18-192 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 18-193 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		

Table 18-193 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 18-194 PoolDepleted

Alarm	Attributes	Applicable major release
Name: PoolDepleted (3950) Type: configurationAlarm Package: dhcp.PoolDepleted Raised on class: dhcp.AddressPool	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Address pool becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a pool becomes zero. Please increase the pool address range or create another address pool.		

Table 18-195 PoolMinFreeExc

Alarm	Attributes	Applicable major release
Name: PoolMinFreeExc (3696) Type: configurationAlarm Package: dhcp.PoolMinFreeExc Raised on class: dhcp.AddressPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowPoolMin	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		
Remedial action: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		

Table 18-196 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol- dExceededAlarm	Release: • 10.0 • 11.0 • 12.0

Table 18-196 PortEtherSymMonSDAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 18-197 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 18-198 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 10.0 • 11.0 • 12.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-199 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 10.0 • 11.0 • 12.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-200 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-201 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 10.0 • 11.0 • 12.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		

Table 18-201 PowerSupplyInputFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-202 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 18-203 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 10.0 • 11.0 • 12.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-204 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 10.0 • 11.0 • 12.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-205 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 18-206 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 18-207 PppoeNcpFailure

Alarm	Attributes	Applicable major release
Name: PppoeNcpFailure (8410) Type: processingErrorAlarm Package: service.PppoeNcpFailure Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapPppoeNcpFailure	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates there is a NCP phase setup problem.		
Remedial action: This alarm indicates the NCP phase setup failed, thus IP protocol can not be configured for the user that attempted to set up the PPPoE session. Please verify NCP setup configuration.		

Table 18-208 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 18-209 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 18-210 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 18-211 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 18-212 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 18-213 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 18-214 RadiusAcctPlcyFailure

Alarm	Attributes	Applicable major release
Name: RadiusAcctPlcyFailure (363) Type: radiusAccountingPolicyAlarm Package: radiusaccounting.RadiusAcctPlcyFailure Raised on class: radiusaccounting.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: radiusAccountingRequestFailure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a RADIUS accounting request is not successfully sent to any of the RADIUS servers specified in the RADIUS accounting policy.		
Remedial action: The Radius server(s) which are configured in the accounting policy are unreachable. This may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the Radius server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 18-215 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 18-216 radiusServerOutOfService (subscrauth)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: subscrauth.radiusServerOutOfService Raised on class: subscrauth.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: subAuthPlcyRadSerOper-StatChg	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the subscriber authentication policy.		

Table 18-217 radiusServerOutOfService (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: radiusaccounting.radiusServerOutOfService Raised on class: radiusaccounting.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radAcctPlcyRadSerOper-StatChg	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the RADIUS accounting policy.		

Table 18-218 radiusServerOverloaded (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOverloaded (3913) Type: communicationsAlarm Package: radiusaccounting.radiusServerOverloaded Raised on class: radiusaccounting.RadiusEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusServerRequestLimi-tReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the RADIUS server is overloaded.		
Remedial action: Verify the RADIUS server is properly configured to process pending accounting requests at the desired rate and ensure that this rate matches the accounting request limit defined for this RADIUS server on the RADIUS accounting policy.		

Table 18-219 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 18-220 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 18-221 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		

Table 18-221 RedundantMepMissing (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 18-222 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 18-223 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 18-224 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 18-225 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-226 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		

Table 18-226 RouteDistinguisherNotConfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 18-227 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 18-228 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 18-229 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 18-230 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 18-231 SapSubAuthError

Alarm	Attributes	Applicable major release
Name: SapSubAuthError (8411) Type: processingErrorAlarm Package: service.SapSubAuthError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 18-232 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 18-233 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 18-234 scriptBackupLost

Alarm	Attributes	Applicable major release
Name: scriptBackupLost (273) Type: configurationAlarm Package: subscrident.scriptBackupLost Raised on class: subscrident.Policy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the primary subscriber identification script URL is operationally up, but a lower-priority script or URL is operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' EQUAL 'Up') AND (('Secondary Script Operational State' NOT EQUAL 'Up') OR ('Tertiary Script Operational State' NOT EQUAL 'Up')))		

Table 18-234 scriptBackupLost (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' NOT EQUAL 'Up') OR (('Secondary Script Operational State' EQUAL 'Up') AND ('Tertiary Script Operational State' EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 18-235 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 18-236 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 18-237 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 18-238 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 18-239 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		

Table 18-239 SectionB1Error (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-240 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 18-241 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 18-242 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-243 ServerDeclineStaticAddr

Alarm	Attributes	Applicable major release
Name: ServerDeclineStaticAddr (3951) Type: configurationAlarm Package: dhcp.ServerDeclineStaticAddr Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpClientHasStaticIpAddress	Release: • 10.0 • 11.0 • 12.0
Description: The tmnxDhcpSvrDeclineStaticAddr notification is generated when a DHCP decline message is received from a DHCP client that has a static IP address assigned.		
Remedial action: DHCP client has a static IP address. Make sure that the DHCP client has a dynamic IP address		

Table 18-244 ServerUserDatabaseUnknown

Alarm	Attributes	Applicable major release
Name: ServerUserDatabaseUnknown (3952) Type: configurationAlarm Package: dhcp.ServerUserDatabaseUnknown Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CannotFindUserDatabase	Release: • 10.0 • 11.0 • 12.0
Description: The tmnxDhcpSvrUserDbUnknown notification is generated when the local DHCP server instance drops a DHCP message because a local user database with the name specified for this server instance could not be found.		
Remedial action: Please specify a valid local user database for this server instance.		

Table 18-245 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 18-246 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 18-247 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 18-247 ShamLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-248 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 18-249 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-250 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-251 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-252 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		

Table 18-252 SonetPathLossOfPointer (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-253 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment. SonetPathPayloadMismatch Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 18-254 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 18-255 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment. SonetPathRemoteDefectIndication Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-256 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment. SonetPathUnequippedPathError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-257 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0

Table 18-257 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 18-258 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 18-259 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 18-260 SubHostLcktLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktLimitReached (4387) Type: configurationAlarm Package: netw.SubHostLcktLimitReached Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when the system wide maximum number of lockout hosts is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout.		

Table 18-261 SubHostLcktSapLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktSapLimitReached (4391) Type: configurationAlarm Package: service.SubHostLcktSapLimitReached Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktSapLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when the maximum number of lockout hosts on a given SAP is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout on the SAP.\n3. Change the Maximum Lockout Hosts (per SAP).		

Table 18-262 SubMcsRelatedProblem

Alarm	Attributes	Applicable major release
Name: SubMcsRelatedProblem (8404) Type: processingErrorAlarm Package: netw.SubMcsRelatedProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subMcsRelatedProblem	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when a subscriber management specific problem occurs during Multi Chassis Syncing, e.g. of DHCP lease states.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 18-263 SubnetDepleted

Alarm	Attributes	Applicable major release
Name: SubnetDepleted (3953) Type: configurationAlarm Package: dhcp.SubnetDepleted Raised on class: dhcp.Subnet	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Subnet becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a subnet becomes zero. Please create another subnet.		

Table 18-264 SubnetMinFreeExc

Alarm	Attributes	Applicable major release
Name: SubnetMinFreeExc (516) Type: configurationAlarm Package: dhcp.SubnetMinFreeExc Raised on class: dhcp.Subnet	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowSubnet-Min	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the actual number of free addresses in a subnet falls below the desired minimum number specified in the subnet configuration		
Remedial action: Please ensure that an adequate free address threshold is configured or create a new subnet to meet the system requirements. \nThis warning is raised on IPv4 DHCP servers only.		

Table 18-265 SubRadSapCoAError

Alarm	Attributes	Applicable major release
Name: SubRadSapCoAError (8416) Type: processingErrorAlarm Package: service.SubRadSapCoAError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: changeOfAddressError	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates that system was unable to process a Change of Authorization (CoA) request from a Radius server.		
Remedial action: Please ensure that Accept CoA attribute is properly enabled on the subscriber authentication policy defined for the service. Ensure that the object targeted by the CoA request (a subscriber host for example) is present on the router.		

Table 18-266 SubscriberAuthError (vprn)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: vprn.SubscriberAuthError Raised on class: vprn.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 18-267 SubscriberAuthError (ies)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: ies.SubscriberAuthError Raised on class: ies.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 18-268 SubscriberInterfaceDown

Alarm	Attributes	Applicable major release
Name: SubscriberInterfaceDown (440) Type: SubscriberInterfaceAlarm Package: service.SubscriberInterfaceDown Raised on class: service.SubscriberInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a subscriber interface is operationally down. The alarm clears when the subscriber interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 18-269 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 18-270 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 18-271 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 18-272 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 18-273 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 18-274 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		

Table 18-274 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 18-275 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 10.0 • 11.0 • 12.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 18-276 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 10.0 • 11.0 • 12.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 18-277 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 18-278 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		

Table 18-278 TunnelAdministrativelyDown (svt) (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 18-279 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 18-280 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 18-281 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment.TxSectionSynchronizationError Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 18-282 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 18-283 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		

Table 18-283 UnmanageFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 18-284 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 18-285 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 18-286 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 18-287 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 18-288 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 18-289 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-290 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 18-291 WppHostAuthenticationFailed

Alarm	Attributes	Applicable major release
Name: WppHostAuthenticationFailed (3916) Type: processingErrorAlarm Package: wpp.WppHostAuthenticationFailed Raised on class: wpp.Portal	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: portalWppHostAuthentication-Failure	Release: • 10.0 • 11.0 • 12.0

Table 18-291 WppHostAuthenticationFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a WPP host cannot be authenticated.		
Remedial action: The recovery action will depend on the exact failure cause as given by the failureReason.		

Table 18-292 WppPortalUnreachable

Alarm	Attributes	Applicable major release
Name: WppPortalUnreachable (5421) Type: ProtocolAlarm Package: wpp.WppPortalUnreachable Raised on class: wpp.Portal	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: protocolDown	Release: • 12.0
Description: This alarm is raised when WPP protocol messages are sent out after a node is restarted but no route to the web portal is available. This notification is sent every minute while the portal remains unreachable up to a certain time. After that, all WPP messages to that portal are dropped.		
Remedial action: Initially no recovery is required as it is expected that the WPP portal can be unreachable for some time after a node restart. When the problem remains, the operator should check the routing table.		

Table 18-293 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 18-294 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 10.0 • 11.0 • 12.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		

Table 18-294 XplError (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

19 7750 SR

19.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 19-1 AaPolicerResourcesExceeded

Alarm	Attributes	Applicable major release
Name: AaPolicerResourcesExceeded (2930) Type: configurationAlarm Package: aapolicy.AaPolicerResourcesExceeded Raised on class: aapolicy.AaSubOvrd	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AaPolicerResourcesExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Application Assurance configured override values exceed policer resources.		
Raising condition: (('Policer Resource Status' EQUAL 'Exceeded'))		
Clearing condition: (('Policer Resource Status' NOT EQUAL 'Exceeded'))		
Remedial action: The Application Assurance Subscriber Policy override(s) configuration has exceeded the policer resources. Remove overrides of a policy configuration for an Application Assurance subscriber where this may be occurring. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-2 AarpDown

Alarm	Attributes	Applicable major release
Name: AarpDown (3704) Type: AarpDown Package: aapolicy.AarpDown Raised on class: aapolicy.Aarp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aarpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an AARP is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 19-2 AarpDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The application assurance redundancy protocol is down either because it is administratively disabled, faulty or a peer address is not up. Ensure that the AARP is administratively up, and the peer ip address and this ip address points to each other.		

Table 19-3 AarpInterfaceDown

Alarm	Attributes	Applicable major release
Name: AarpInterfaceDown (3904) Type: AarpInterfaceDown Package: service.AarpInterfaceDown Raised on class: service.AarpInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an AARP interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 19-4 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		

Table 19-4 AccessInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 19-5 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 19-6 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 19-7 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 19-8 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 19-9 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 19-10 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 19-11 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 19-12 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 19-13 AtcaPowerSupplyFailure

Alarm	Attributes	Applicable major release
Name: AtcaPowerSupplyFailure (1125) Type: equipmentAlarm Package: equipment.AtcaPowerSupplyFailure Raised on class: equipment.PowerSupply	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 14.0
Description: The alarm is raised when the associated power supply is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled'))		

Table 19-13 AtcaPowerSupplyFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Enabled')		
Remedial action: Check the status of the site power supply.		

Table 19-14 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 19-15 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 19-16 BackPlaneEPROMFailed

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMFailed (12488) Type: equipmentAlarm Package: netw.BackPlaneEPROMFailed Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access the backplane EPROM due to a hardware defect.		
Remedial action: The active CPM is at risk of failing to initialize after node reboot due to not being able to access the BP EPROM to read the chassis type. Contact Nokia customer support.		

Table 19-17 BackPlaneEPROMWarning

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMWarning (12489) Type: equipmentAlarm Package: netw.BackPlaneEPROMWarning Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access one backplane EPROM due to a hardware defect but a redundant EPROM is present and accessible.		
Remedial action: There is no effect on system operation.No recovery action required.		

Table 19-18 backupScriptInUse

Alarm	Attributes	Applicable major release
Name: backupScriptInUse (274) Type: configurationAlarm Package: subscrident.backupScriptInUse Raised on class: subscrident.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupInUse	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary subscriber identification script is operationally down, but one of the other scripts is operationally up.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND (('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		

Table 19-18 backupScriptInUse (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR (('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 19-19 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 19-20 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 19-21 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 19-22 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 19-23 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 19-24 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 19-25 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-25 BgpDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-26 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 19-27 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 19-28 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 19-29 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 19-30 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-30 BITSNotQualified (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 19-31 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 19-32 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 19-33 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 19-34 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 19-35 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 19-36 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 19-37 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 19-38 CardDegrade

Alarm	Attributes	Applicable major release
Name: CardDegrade (1987) Type: equipmentAlarm Package: equipment.CardDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgr	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Card degrade - device is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Is the alarmed pack a 100G Coherent OT (112SCA1, 112SNA1, 112SCX10 or 112SNX10)? 2. Check the line port information and Line port PM.If the OPT and OPR parameters are blank go to Step 3.3. Check the firmware profile that is currently running on the pack.If not, go to Step 7.If the firmware profile for the card is lower than the versions shown in the table below,then the firmware should be upgraded see - Selecting a Specific Firmware Version 4. Perform a cold reset of the card.5. Reseat the card.6. Replace the card.7. Perform a warm reset of the card.		

Table 19-39 CcagDown

Alarm	Attributes	Applicable major release
Name: CcagDown (210) Type: equipmentAlarm Package: ccag.CcagDown Raised on class: ccag.CrossConnectAggregationGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CcagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the CCAG Administrative State is Up and the Operational State is Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 19-40 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-41 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-41 CesBfrUnderrun (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-42 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-43 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-44 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-45 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-46 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-47 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 19-48 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 19-49 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 19-50 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 19-51 CoherentOpticalModuleFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleFault (4612) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ModuleFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports module fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault')))		
Remedial action: Module Fault occurred.		

Table 19-52 CoherentOpticalModuleHostTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleHostTxFault (4613) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleHostTxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleHostTxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Host Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit'))		

Table 19-52 CoherentOpticalModuleHostTxFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit')))		
Remedial action: Module Host Tx Fault occurred.		

Table 19-53 CoherentOpticalModuleReferenceLockLoss

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleReferenceLockLoss (4614) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleReferenceLockLoss Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceLockLoss	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports loss of reference lock signal on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module')))		
Remedial action: Loss of reference lock.		

Table 19-54 CoherentOpticalModuleRxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleRxFault (4615) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleRxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleRxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Rx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive')))		
Remedial action: Module Rx Fault occurred.		

Table 19-55 CoherentOpticalModuleTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleTxFault (4616) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleTxFault Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleTxFault	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit')))		
Remedial action: Module Tx Fault occurred.		

Table 19-56 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 19-57 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		

Table 19-57 ConfigurationRescueFileSaveStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 19-58 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 19-59 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 19-60 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback. ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 19-61 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 19-62 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 19-63 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 19-64 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 19-65 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		

Table 19-65 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 19-66 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 19-67 ControlChannelDown

Alarm	Attributes	Applicable major release
Name: ControlChannelDown (8390) Type: ProtocolAlarm Package: Imp.ControlChannelDown Raised on class: Imp.ControlChannel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when a Control Channel has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A network configuration issue has been detected. Ensure the Control Channel configuration between the local node and the peer node is consistent.		

Table 19-68 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 19-69 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-70 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-71 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-72 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtVioIPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-72 CpmProtectionViolationPortEntry (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-73 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-74 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 19-75 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 19-76 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec. CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 19-77 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		

Table 19-77 DDMAux1HighAlarm (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-78 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-79 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-80 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-81 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-82 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-82 DDMAux2HighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-83 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-84 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-85 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-86 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-87 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-87 DDMRxOpticalPowerLowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-88 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-89 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-90 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-91 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-92 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-92 DDMSupplyVoltageLowWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-93 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-94 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-95 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-96 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-97 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-97 DDMTxBiasCurrentHighAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-98 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-99 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-100 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-101 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-102 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-102 DDMTxOutputPowerHighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-103 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-104 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 19-105 DeterministicNatMapOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatMapOperDown (9570) Type: equipmentAlarm Package: nat.DeterministicNatMapOperDown Raised on class: nat.DeterministicNatMap	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatMapOper-Down	Release: • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Map is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 19-106 DeterministicNatPrefixOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatPrefixOperDown (9571) Type: equipmentAlarm Package: nat.DeterministicNatPrefixOperDown Raised on class: nat.DeterministicNatPrefix	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatPrefixOper-Down	Release: • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Prefix is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'InService') AND ('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 19-107 DhcpLseStateMobilityError

Alarm	Attributes	Applicable major release
Name: DhcpLseStateMobilityError (8409) Type: configurationAlarm Package: service.DhcpLseStateMobilityError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapDHCPLseStateMobilityEr-ror	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system was unable to perform a mobility check for this lease state.		
Remedial action: Please make sure that host-connectivity-verify is enabled on the SAP.		

Table 19-108 DhcpLseStateRestoreProblem

Alarm	Attributes	Applicable major release
Name: DhcpLseStateRestoreProblem (8402) Type: processingErrorAlarm Package: netw.DhcpLseStateRestoreProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpLseStateRestoreProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when an error is detected while processing a persistency record.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 19-109 DhcpMiscellaneousProblem

Alarm	Attributes	Applicable major release
Name: DhcpMiscellaneousProblem (8403) Type: processingErrorAlarm Package: netw.DhcpMiscellaneousProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpMiscellaneousProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a miscellaneous DHCP problem occurs.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 19-110 DHCPPoolFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPPoolFailoverStateChange (5168) Type: configurationAlarm Package: dhcp.DHCPPoolFailoverStateChange Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPPoolFailoverStat-eChanged	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Local DHCP Pool Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		

Table 19-110 DHCPPoolFailoverStateChange (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the operational state of a particular Local DHCP Pool Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a pool failover is in progress.\nThis alarm is cleared implicitly when the DHCP Pool Failover state returns to Normal.		

Table 19-111 DHCPServerFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPServerFailoverStateChange (4986) Type: configurationAlarm Package: dhcp.DHCPServerFailoverStateChange Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPServerFailoverStat-eChanged	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Local DHCP Server Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when operational state of a particular Local DHCP Server Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a server failover is in progress.\nThis alarm will be cleared implicitly when the DHCP Server Failover state returns to Normal.		

Table 19-112 DHCPSFoLeaseUpdateFailedAddressConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedAddressConflict (4977) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedAddressConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedAddressConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a address conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased another address to this host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased another address to this host. Please ensure all configuration is correct.		

Table 19-113 DHCPSFoLeaseUpdateFailedfoShutdown

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedfoShutdown (4985) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedfoShutdown Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedfoShutdown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a shutdown lease update received from the failover peer cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'. Please ensure all configuration is correct.		

Table 19-114 DHCPSFoLeaseUpdateFailedHostConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedHostConflict (4978) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedHostConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedHostConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a host conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased this address to another host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased this address to another host. Please ensure all configuration is correct.		

Table 19-115 DHCPSFoLeaseUpdateFailedLeaseExpired

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedLeaseExpired (4979) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedLeaseExpired Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedLeaseExpired	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-115 DHCPSFoLeaseUpdateFailedLeaseExpired (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when a lease expired lease update received from the failover peer cannot be processed successfully. The lease received from the peer has expired.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer has expired. Please ensure all configuration is correct.		

Table 19-116 DHCPSFoLeaseUpdateFailedMaxLeaseReached

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedMax-LeaseReached (4980) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedMaxLeaseReached Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedMaxLeaseReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a maximum reached lease update received from the failover peer cannot be processed successfully. The maximum number of leases is already reached.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The maximum number of leases is already reached. Please ensure all configuration is correct.		

Table 19-117 DHCPSFoLeaseUpdateFailedPeerConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPeerConflict (4981) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPeerConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPeerConflict	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a peer conflict lease update received from the failover peer cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance. Please ensure all configuration is correct.		

Table 19-118 DHCPSFoLeaseUpdateFailedPersistenceCongested

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPersistenceCongested (4982) Type: configurationAlarm Package: dhcp.DHCPSFoLeaseUpdateFailedPersistenceCongested Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFailedPersistenceCongested	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a persistence congested lease update received from the failover peer cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload. Please ensure all configuration is correct.		

Table 19-119 DHCPSFoLeaseUpdateFailedRangeNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedRangeNotFound (4983) Type: configurationAlarm Package: dhcp.DHCPSFoLeaseUpdateFailedRangeNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFailedRangeNotFound	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a range not found lease update received from the failover peer cannot be processed successfully. No valid include range for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid include range for this lease could be found. Please ensure all configuration is correct.		

Table 19-120 DHCPSFoLeaseUpdateFailedSubnetNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedSubnetNotFound (4984) Type: configurationAlarm Package: dhcp.DHCPSFoLeaseUpdateFailedSubnetNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFailedSubnetNotFound	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a subnet not found lease update received from the failover peer cannot be processed successfully. No valid subnet for this lease could be found.		

Table 19-120 DHCPSFoLeaseUpdateFailedSubnetNotFound (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid subnet for this lease could be found. Please ensure all configuration is correct.		

Table 19-121 DhcpSvrNoSubnetFixAddr

Alarm	Attributes	Applicable major release
Name: DhcpSvrNoSubnetFixAddr (8378) Type: configurationAlarm Package: dhcp.DhcpSvrNoSubnetFixAddr Raised on class: dhcp.LocalDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dhcpSvrNoSubnetFixAddr	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm can be generated for hosts configured with a fixed IP address in the local user database. If such a host requests an ip-address and the system cannot find a matching subnet in this server instance for this IP address, then this alarm is generated, and the request is dropped.		
Remedial action: Ensure that the IP Address configured for this host under the local user database falls into a subnet under the local DHCP server mapped to this alarm.		

Table 19-122 DiamAppMessageDropped

Alarm	Attributes	Applicable major release
Name: DiamAppMessageDropped (5175) Type: processingErrorAlarm Package: diameter.DiamAppMessageDropped Raised on class: diameter.DiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamAppMessageDropped	Release: • 12.0 • 13.0
Description: The alarm is raised when the Diameter protocol has dropped a message		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 19-123 DiamProxyOperationalStateChange

Alarm	Attributes	Applicable major release
Name: DiamProxyOperationalStateChange (8427) Type: communicationsAlarm Package: diameter. DiamProxyOperationalStateChange Raised on class: diameter.DiameterPeerProxy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiameterProxyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a Diameter Peer Proxy is Out Of Service.		
Raising condition: ('Operational State' EQUAL 'Out Of Service')		
Clearing condition: ('Operational State' EQUAL 'in Service')		
Remedial action: Please ensure that the Diameter Peer Proxy on Diameter Policy is operationally up.		

Table 19-124 DiscoveredPhysicalLinkMismatch

Alarm	Attributes	Applicable major release
Name: DiscoveredPhysicalLinkMismatch (657) Type: configurationAlarm Package: netw.DiscoveredPhysicalLinkMismatch Raised on class: netw.AbstractPhysicalLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: endPointUsedByNumerou-sLinks	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one endpoint of a physical link is used as an endpoint in another physical link.		
Raising condition: ('physicalLinkMismatchConfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMismatchConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. Physical link endpoint (i.e. ports) can only be configured in one link.		

Table 19-125 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-125 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 19-126 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 19-127 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 19-128 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 19-129 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 19-130 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment.DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-130 DS1E1ResourceAvailabilityIndicator (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 19-131 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 19-132 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 19-133 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 19-134 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 19-135 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 19-136 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 19-137 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-137 DS3E3ResourceAvailability (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 19-138 DuplicatePhysicalLinks

Alarm	Attributes	Applicable major release
Name: DuplicatePhysicalLinks (658) Type: configurationAlarm Package: netw.DuplicatePhysicalLinks Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicatePhysicalLinkConfig-ured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is more then one physical link configured between two endpoints.		
Raising condition: ('duplicateLinkConfigured' EQUAL 'true')		
Clearing condition: ('duplicateLinkConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The duplicated link must be deleted.		

Table 19-139 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		

Table 19-139 EfmOamAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 19-140 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 19-141 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 19-142 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 19-143 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-144 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 19-145 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 19-146 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-146 EquipmentRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 19-147 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 19-148 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 19-149 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 19-150 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 19-151 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 19-152 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 19-153 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 19-154 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 19-155 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 19-156 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 19-157 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 19-158 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 19-159 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-159 FanTrayRemoved (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 19-160 FirmwareErrorAlarm

Alarm	Attributes	Applicable major release
Name: FirmwareErrorAlarm (11087) Type: firmwareAlarm Package: equipment.FirmwareErrorAlarm Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: firmwareError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the device installed in the shelf has an EEPROM that does not contain the correct or recognizable information.		
Remedial action: The alarm is raised when the device installed in the shelf has an EEPROM that does not contain the correct or recognizable information. Replace the card.		

Table 19-161 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 19-162 FpgaFail

Alarm	Attributes	Applicable major release
Name: FpgaFail (4485) Type: equipmentAlarm Package: equipment.FpgaFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAFAIL	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when FPGA download failure is detected.		
Remedial action: 1 Perform a warm reset on the card where the FPGAFAIL condition is raised.\nFor CLI config card card type shelf slot reset warm.\nFor WEBUI Select the card, click the Reboot tab, select Warm Reboot >Submit.\n2 Contact your Nokia support representative.		

Table 19-163 FpgaTimeout

Alarm	Attributes	Applicable major release
Name: FpgaTimeout (4487) Type: equipmentAlarm Package: equipment.FpgaTimeout Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGATIMEOUT	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when FPGA timeout is detected.		
Remedial action: 1. Perform a warm reset on the card where the FPGATIMEOUT condition is raised.		

Table 19-164 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		

Table 19-164 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 19-165 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 19-166 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 19-167 GmplsLspDown

Alarm	Attributes	Applicable major release
Name: GmplsLspDown (8383) Type: pathAlarm Package: gmplsuni.GmplsLspDown Raised on class: gmplsuni.GmplsLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmplsLspDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS LSP's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS LSP's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS LSP is down, despite the Administrative state being up. Check if the GMPLS path, or the LSP-path binding is down.		

Table 19-168 GmplsLspPathBindingDown

Alarm	Attributes	Applicable major release
Name: GmplsLspPathBindingDown (8384) Type: pathAlarm Package: gmplsuni.GmplsLspPathBindingDown Raised on class: gmplsuni.LspPathBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmplsLspPathBindingDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS LSP-path binding's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS LSP-path binding's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS LSP-path binding is down, despite the Administrative state being up. Check the failure code and fix accordingly.		

Table 19-169 GRETunnelDown

Alarm	Attributes	Applicable major release
Name: GRETunnelDown (3326) Type: serviceAlarm Package: svt.GRETunnelDown Raised on class: svt.GRETunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IP/GRE tunnel Operational State changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		

Table 19-169 GRETunnelDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The situation may occur if the underlying physical port is down either because of administrative disabling or a fault on the port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable.		

Table 19-170 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 19-171 GroupInterfaceDown

Alarm	Attributes	Applicable major release
Name: GroupInterfaceDown (441) Type: GroupInterfaceAlarm Package: service.GroupInterfaceDown Raised on class: service.GroupInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a group interface is operationally down. The alarm clears when the group interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 19-172 HostConnectivityLostRateExceeded

Alarm	Attributes	Applicable major release
Name: HostConnectivityLostRateExceeded (276) Type: communicationsAlarm Package: ressubscr.HostConnectivityLostRateExceeded Raised on class: ressubscr.ShcvSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hostDown Applicable probable causes: • hostDown • trapDropped	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the trapDroppedRaisesAlarm parameter is enabled and the maximum allowed number of SHCV host connectivity loss events on a SAP is exceeded. The SHCV action in response to the alarm is specified by the maxHostLostConnectivityRate parameter. If the specified action is to remove the host information, the host information is removed and the connectivity of the host is not subsequently verified.		
Remedial action: This may be a transient error condition in the network or possible congestion or could be a sign that the SHCV ping interval is too short. Verify the status of the network for those subscribers and the service SHCV configuration.		

Table 19-173 IGHMisconfigured

Alarm	Attributes	Applicable major release
Name: IGHMisconfigured (827) Type: ighAlarm Package: igh.IGHMisconfigured Raised on class: igh.InterfaceGroupHandler	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IGHProtocolMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IGH is administratively up but none of the IGH protocols is operationally up.		
Raising condition: (('igh_misconfigured' EQUAL '\"yes\"') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('igh_misconfigured' NOT EQUAL '\"yes\"') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Please check the configuration.		

Table 19-174 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-174 IgmpDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 19-175 IgmpMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxGrpSrcsLimitExceeded (4624) Type: configurationAlarm Package: igmp.IgmpMaxGrpSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Needs to increase 'maxGrpSources' value to allow more sources on this interface.		

Table 19-176 IgmpMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxSrcsLimitExceeded (3742) Type: configurationAlarm Package: igmp.IgmpMaxSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxSrcsLimitExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP source for a group when the number of sources for this group is equal to 'maxSources', the maximum number of sources per group supported on the interface.		
Remedial action: Needs to increase 'maxSources' value to allow more sources on this interface.		

Table 19-177 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 19-178 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 19-179 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 19-180 IncorrectNeighborConfig

Alarm	Attributes	Applicable major release
Name: IncorrectNeighborConfig (609) Type: configurationAlarm Package: aps.IncorrectNeighborConfig Raised on class: aps.ApsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incorrectNeighborConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.		
Raising condition: (('Type' EQUAL 'MultiChassis') AND ('Neighbor match' EQUAL 'false'))		
Clearing condition: (('Type' EQUAL 'SingleChassis') OR ('Neighbor match' EQUAL 'true'))		
Remedial action: Make sure a peer exist and the neighbor address points to a network interface on the NE that contains the peer object.		

Table 19-181 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 19-182 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 19-183 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 19-184 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 19-185 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-185 InstanceDown (vrrp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 19-186 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 19-187 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 19-188 InterfaceDown (service)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: service.InterfaceDown Raised on class: service.RedundantInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a redundant interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 19-189 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 19-190 InterfaceDown (vprn)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vprn.InterfaceDown Raised on class: vprn.IPMirrorInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 19-191 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-192 IntTempLow

Alarm	Attributes	Applicable major release
Name: IntTempLow (3361) Type: equipmentAlarm Package: equipment.IntTempLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempLow	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Card under temperature is detected.		
Remedial action: Ensure that no environmental issues are present where the network element resides.Resolve any existing issues.Verify if other cards in the shelf report temperatures near their lower limit (within 10ï¿½ C).Replace the alarmed card.		

Table 19-193 IOMEventOverflow

Alarm	Attributes	Applicable major release
Name: IOMEventOverflow (5617) Type: equipmentAlarm Package: equipment.IOMEventOverflow Raised on class: equipment.BaseCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMEventOverflow	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is generated when tmnxIomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimitReached occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.		
Remedial action: Informational - The alarm will be cleared when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.		

Table 19-194 IOMResUtilizationLimit

Alarm	Attributes	Applicable major release
Name: IOMResUtilizationLimit (5618) Type: equipmentAlarm Package: equipment.IOMResUtilizationLimit Raised on class: equipment.BaseCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMResHighLimitReached Applicable probable causes: • IOMResHighLimitReached • IOMResExhausted	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the value of tmnxIomResourceLimitPct.		
Remedial action: Informational - The alarm will be cleared when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.		

Table 19-195 IPSecGatewayDown

Alarm	Attributes	Applicable major release
Name: IPSecGatewayDown (830) Type: serviceAlarm Package: ipsec.IPSecGatewayDown Raised on class: ipsec.IPSecGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: gatewayDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a SAP IPsec gateway changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 19-196 IPSecIsaGrpDown

Alarm	Attributes	Applicable major release
Name: IPSecIsaGrpDown (3745) Type: equipmentAlarm Package: isa.IPSecIsaGrpDown Raised on class: isa.IPSecIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPSecIsaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA IPSec group is Down and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Tunnel Group is down, despite the administrative state being up. Check that the configured ISA-Tunnel Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application IPSec(Tunnel) Group.		

Table 19-197 IPSecIsaMemoryHigh

Alarm	Attributes	Applicable major release
Name: IPSecIsaMemoryHigh (11089) Type: thresholdCrossed Package: equipment.IPSecIsaMemoryHigh Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The Alarm is generated when the ISA card memory usage ratio has reached the high watermark ,which is measured by the number of phase 1 and phase 2 security associations (SAs).		
Remedial action: This alarm is raised when the ISA card memory usage ratio reaches the high watermark which is measured by the number of phase 1 and phase 2 security associations (SAs). The value used for the high watermark is 95% of the maximum number of SAs for the ISA Card. The alarm is cleared when the ISA card memory usage ratio reaches the low watermark.		

Table 19-198 IPSecIsaMemoryMax

Alarm	Attributes	Applicable major release
Name: IPSecIsaMemoryMax (11090) Type: thresholdCrossed Package: equipment.IPSecIsaMemoryMax Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The Alarm is generated when the ISA card memory usage ratio has reached the Maximum which is measured by the number of phase 1 and phase 2 security associations (SAs).		
Remedial action: This alarm is raised when the ISA card memory usage ratio reaches the maximum value of security associations (SAs) associated with the ISA Card. This maximum value is measured by the number of phase 1 and phase 2 SAs. The alarm is cleared when the number of SAs reaches the low watermark.		

Table 19-199 IPSecTunnelBfdConnectionBroken

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionBroken Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BFD connection to a peer times out.		

Table 19-199 IPSecTunnelBfdConnectionBroken (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 19-200 IPSecTunnelBfdConnectionDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 19-201 IPSecTunnelBfdConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm Package: ipsec. IPSecTunnelBfdConnectionPeerDetectsDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 19-202 IPSecTunnelDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelDown (834) Type: serviceAlarm Package: ipsec.IPSecTunnelDown Raised on class: ipsec.IPSecTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IPsec tunnel operational state changes to 'down' and the administrative state is 'up'.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 19-203 IsaAaGrpDown

Alarm	Attributes	Applicable major release
Name: IsaAaGrpDown (647) Type: equipmentAlarm Package: isa.IsaAaGrpDown Raised on class: isa.AaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an ISA-AA group Operational State is Down, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-AA group is down, despite the administrative state being up. Check that the configured ISA-AA Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Assurance MDA.		

Table 19-204 IsaAaSubUnassigned

Alarm	Attributes	Applicable major release
Name: IsaAaSubUnassigned (836) Type: equipmentAlarm Package: isa.IsaAaSubUnassigned Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaSubUnassigned	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. The unassigned subscriber is treated as specified by the Operation Upon Failure parameter in the AA group. Recovery from this condition requires the removal and recreation of the AA subscriber when sufficient resources are available.		
Raising condition: (('Number of Unassigned ESM Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned SAP Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned Spoke SDP Subscribers' NOT EQUAL '0L'))		
Clearing condition: (('Number of Unassigned ESM Subscribers' EQUAL '0L') AND ('Number of Unassigned SAP Subscribers' EQUAL '0L') AND ('Number of Unassigned Spoke SDP Subscribers' EQUAL '0L'))		
Remedial action: The subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. Remove and recreate the AA subscriber when sufficient resources are available.		

Table 19-205 IsaLnsGrpDown

Alarm	Attributes	Applicable major release
Name: IsaLnsGrpDown (1119) Type: equipmentAlarm Package: isa.IsaLnsGrpDown Raised on class: isa.LnsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaLnsGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA-LNS group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is caused by administrative shutdown or equipment failure of the MDA members. Review the status of the underlying ISA MDA group members and ensure they are operational.		

Table 19-206 IsaVideoGrpDown

Alarm	Attributes	Applicable major release
Name: IsaVideoGrpDown (775) Type: equipmentAlarm Package: isa.IsaVideoGrpDown Raised on class: isa.VideoGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaVideoGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an ISA video group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Video Group is down, despite the administrative state being up. Check that the configured ISA-Video Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Video Group.		

Table 19-207 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 19-208 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 19-209 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 19-210 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-210 KeepAliveProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 19-211 L2TPDown

Alarm	Attributes	Applicable major release
Name: L2TPDown (841) Type: ProtocolAlarm Package: l2tp.L2TPDown Raised on class: l2tp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2TP site becomes administratively down. The alarm clears when the L2TP site becomes administratively up.		
Raising condition: ('Administrative State' EQUAL 'Down')		
Clearing condition: ('Administrative State' EQUAL 'Up')		
Remedial action: This alarm indicates that the L2TP protocol administrative state is down. It is cleared automatically when L2TP administrative state is up again. Please verify the L2TP configuration. This alarm can be safely suppressed if L2TP is not used.		

Table 19-212 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		

Table 19-212 LabelProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 19-213 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 19-214 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 19-215 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 19-216 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 19-217 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-217 LdpTargetedPeerDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 19-218 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 19-219 liMirrorLiNat64SubOperStateDown

Alarm	Attributes	Applicable major release
Name: liMirrorLiNat64SubOperStateDown (11176) Type: equipmentAlarm Package: mirrorli.liMirrorLiNat64SubOperStateDown Raised on class: mirrorli.LiNat64LsnSub	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: liMirrorLiNatLsnSubOperStat-eDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of the NAT64 subscriber is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.		

Table 19-220 liMirrorLiNatL2awSubOperStateDown

Alarm	Attributes	Applicable major release
Name: liMirrorLiNatL2awSubOperStateDown (9567) Type: equipmentAlarm Package: mirrorli. liMirrorLiNatL2awSubOperStateDown Raised on class: mirrorli.LiNatL2AwareSub	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: liMirrorLiNatL2awSubOperStateDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of the NAT L2 Aware subscriber is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.		

Table 19-221 liMirrorLiNatLsnSubOperStateDown

Alarm	Attributes	Applicable major release
Name: liMirrorLiNatLsnSubOperStateDown (9568) Type: equipmentAlarm Package: mirrorli.liMirrorLiNatLsnSubOperStateDown Raised on class: mirrorli.AbstractLiNatLsnSub	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: liMirrorLiNatLsnSubOperStat-eDown	Release: • 10.0 • 13.0
Description: The alarm is raised when the Operational State of the NAT LSN subscriber is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.		

Table 19-222 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		

Table 19-222 LineAlarmIndicationSignal (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 19-223 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-224 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment. LineRemoteDefectIndication Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		

Table 19-224 LineRemoteDefectIndication (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 19-225 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 19-226 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 19-227 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 19-228 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 19-229 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment.LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 11.0 • 12.0 • 13.0 • 14.0

Table 19-229 LowTemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 19-230 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 19-231 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		

Table 19-231 LspPathBypassTunnelActive (continued)

Alarm	Attributes	Applicable major release
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 19-232 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 19-233 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 19-234 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 19-235 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 19-236 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-236 macMoveRateExceededNonBlock (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 19-237 McIPsecPeerTunnelGroupMissing

Alarm	Attributes	Applicable major release
Name: McIPsecPeerTunnelGroupMissing (4815) Type: configurationAlarm Package: multichassis. McIPsecPeerTunnelGroupMissing Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC IPsec tunnel group. This can be either the peer tunnel group is misconfigured or the local peer group ID is not configured.		
Raising condition: ('peerTunnelGroupPointer' EQUAL '\"\"')		
Clearing condition: ('peerTunnelGroupPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC IPsec tunnel group or check the local tunnel group's peer group ID has been configured, or delete this one if it is not used.		

Table 19-238 McIPsecTunnelGroupDown

Alarm	Attributes	Applicable major release
Name: McIPsecTunnelGroupDown (4816) Type: redundancyAlarm Package: multichassis.McIPsecTunnelGroupDown Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipsecTunnelGroupDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MC IPsec tunnel group is operationally down while it is administratively up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check if the physical ISA IPsec Tunnel Group or the associated MDA is operationally down.		

Table 19-239 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis.MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 19-240 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 19-241 McOmcrStatFailedChanged

Alarm	Attributes	Applicable major release
Name: McOmcrStatFailedChanged (8058) Type: communicationsAlarm Package: multichassis.McOmcrStatFailedChanged Raised on class: multichassis.McOmcrStat	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: McOmcrStatFailedChanged	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the value of the object tmnxMcOmcrStatFailed changes from 'notAct' to any of the other values. The alarm is cleared when the value of the object tmnxMcOmcrStatFailed changes to 'notAct' from any of the other values. A transition from 'notAct' or 'no' to 'yes' means that the traffic of some or all associated client application entries' is being dropped. For example, all traffic from some or all of the IPOE subscriber hosts protected by a failed SRRP instance is dropped by this system. A transition to 'no' means that the system has successfully allocated resources for the traffic of all associated client application entries. A transition to 'notAct' means that this system is not performing the active role anymore for this access protection instance. For example, the value of the object tmnxSrrpOperState has become different from 'master' for the corresponding instance.		
Raising condition: ('Instance Failed' NOT EQUAL 'Not Act')		
Clearing condition: ('Instance Failed' EQUAL 'Not Act')		
Remedial action: There are three recovery actions possible, depending on the reason of the transition of the access protection instance. If it is caused by a problem in the access network, fix that problem, or make additional resources available for this access protection instance. If it is caused by a misconfiguration of this system, correct that, or make additional resources available for this access protection instance.		

Table 19-242 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC endpoint is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 19-243 MemberDown

Alarm	Attributes	Applicable major release
Name: MemberDown (8385) Type: communicationsAlarm Package: gmplsuni.MemberDown Raised on class: gmplsuni.TunnelGroupEndpointMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MemberDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS tunnel group endpoint member's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS tunnel group endpoint member's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS tunnel group endpoint member is down, despite the Administrative state being up. Check with the Reason Down Flags for more details.		

Table 19-244 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 19-245 MepFacilityFault (lag)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: lag.MepFacilityFault Raised on class: lag.Interface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-245 MepFacilityFault (lag) (continued)

Alarm	Attributes	Applicable major release
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 19-246 MepFacilityFault (rtr)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: rtr.MepFacilityFault Raised on class: rtr.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 19-247 MepFacilityFault (equipment)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: equipment.MepFacilityFault Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 19-248 MepFacilityFault (service)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: service.MepFacilityFault Raised on class: service.AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 19-249 MgwPeerConnectionStateAlarm

Alarm	Attributes	Applicable major release
Name: MgwPeerConnectionStateAlarm (4399) Type: connectionStateChangeAlarm Package: wlangw.MgwPeerConnectionStateAlarm Raised on class: wlangw.MgwPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MgwPeerConnection-StateAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the state of a connection with a Mobile Gateway has changed. [CAUSE] The state of a connection with a Mobile Gateway has changed to Fault. [EFFECT] The effect depends on the new state. [RECOVERY] No recovery is required on this system.		
Remedial action: Fault occurred on the connection with Mobile Gateway. Check the physical connection and interfaces between Mobile Gateway and WLAN Gateway.		

Table 19-250 MigrationCompleted

Alarm	Attributes	Applicable major release
Name: MigrationCompleted (753) Type: migrationComplete Package: equipment.MigrationCompleted Raised on class: equipment.NeCardSwapTask	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationComplete	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-250 MigrationCompleted (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a card migration event completes.		
Raising condition: ('Status' EQUAL 'Migration completed')		
Remedial action: Informational - no corrective action required.		

Table 19-251 MigrationFailed

Alarm	Attributes	Applicable major release
Name: MigrationFailed (754) Type: migrationFailure Package: equipment.MigrationFailed Raised on class: equipment.NeCardSwapTask	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a card migration event fails.		
Raising condition: (('Status' EQUAL 'Failed - Latest configuration not available') OR ('Status' EQUAL 'Failed - Unable to migrate configuration') OR ('Status' EQUAL 'Failed - Unable to transfer migrated configuration') OR ('Status' EQUAL 'Failed - Unable to reboot network element'))		
Remedial action: This alarm is raised when a card migration fails. The operation has failed for one of the following reasons - a configuration backup could not be created, the configuration transfer failed or the attempt to reboot the card failed. Please re-attempt the migration. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-252 MinFreePfxThDepleted

Alarm	Attributes	Applicable major release
Name: MinFreePfxThDepleted (9032) Type: configurationAlarm Package: dhcp.MinFreePfxThDepleted Raised on class: dhcp.PrefixMinFreeThreshold	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix becomes zero.		
Remedial action: The operator may create additional prefixes in the considered prefix. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 19-253 MinFreePfxThTooLow

Alarm	Attributes	Applicable major release
Name: MinFreePfxThTooLow (9033) Type: configurationAlarm Package: dhcp.MinFreePfxThTooLow Raised on class: dhcp.PrefixMinFreeThreshold	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesTooLow	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the considered prefix is becoming too low.		
Remedial action: The operator may create additional prefixes in the considered prefix to prevent a shortage of available prefixes with minimum free threshold length. \nAlternatively, examination of the leases in the prefix may reveal that the distribution is not appropriate.		

Table 19-254 MinFreePoolThDepleted

Alarm	Attributes	Applicable major release
Name: MinFreePoolThDepleted (9034) Type: configurationAlarm Package: dhcp.MinFreePoolThDepleted Raised on class: dhcp.AddressPoolMinFreeThreshold	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the pool becomes zero.		
Remedial action: The operator may create additional prefixes in the pool. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 19-255 MinFreePoolThTooLow

Alarm	Attributes	Applicable major release
Name: MinFreePoolThTooLow (9035) Type: configurationAlarm Package: dhcp.MinFreePoolThTooLow Raised on class: dhcp.AddressPoolMinFreeThreshold	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: freePrefixesTooLow	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This Alarm is generated when the actual number of free prefixes with minimum free threshold length available in the pool is becoming too low.		

Table 19-255 MinFreePoolThTooLow (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please create additional prefixes in the pool to prevent a shortage of available prefixes with minimum free threshold length. \nAlternatively, examination of the leases in the pool may reveal that the distribution is not appropriate.		

Table 19-256 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 19-257 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 19-258 MldMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxGrpSrcsLimitExceeded (5395) Type: configurationAlarm Package: mld.MldMaxGrpSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an MLD group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Increase the value of the 'Maximum Number of Group Sources' attribute in the parent MLD interface so that the number of active MLD group sources stays under the configured threshold.		

Table 19-259 MldMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxSrcsLimitExceeded (5396) Type: configurationAlarm Package: mld.MldMaxSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxSrcsLimitExceeded	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an MLD source for a group when the number of sources for this group is equal to 'maxSources', the Maximum Number of Sources per group supported on the interface.		
Remedial action: Increase 'Maximum Number Of Sources' value to allow more sources on this interface.		

Table 19-260 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 19-260 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 19-261 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 19-262 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 19-263 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 19-264 MsdpDown

Alarm	Attributes	Applicable major release
Name: MsdpDown (353) Type: ProtocolAlarm Package: msdp.MsdpDown Raised on class: msdp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the MSDP site.		

Table 19-265 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 19-266 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 19-267 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-267 MvrConfiguredFromVplsNotExist (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 19-268 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 19-269 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 19-270 NatDeterministicChange

Alarm	Attributes	Applicable major release
Name: NatDeterministicChange (5122) Type: configurationAlarm Package: netw.NatDeterministicChange Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatDeterministicMapChanged	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when something changed in the Deterministic NAT map. Such a change may be caused by a modification of the Deterministic NAT Prefix or the Deterministic NAT Map.		
Remedial action: Managers that rely on the offline representation of the Deterministic NAT map should get an updated copy by saving the Deterministic NAT script.		

Table 19-271 NatIsaGrpDegraded

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDegraded (8059) Type: equipmentAlarm Package: nat.NatIsaGrpDegraded Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDegraded	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the NAT ISA group is degraded, while operationally still in service.		
Raising condition: (('Degraded State' EQUAL 'True') AND ('Operational State' EQUAL 'Up'))		
Clearing condition: (('Operational State' NOT EQUAL 'Up') OR ('Degraded State' NOT EQUAL 'True'))		
Remedial action: The ISA-NAT Group is degraded. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 19-272 NatIsaGrpDown

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDown (3887) Type: equipmentAlarm Package: nat.NatIsaGrpDown Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an NAT ISA group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 19-272 NatIsaGrpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the ISA-NAT Group is down, despite the administrative state being up. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 19-273 NatIsaMemberSessionUsageHi

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHi (3937) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHi Raised on class: nat.IsaMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-274 NatIsaMemberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHigh (1070) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHigh Raised on class: nat.IsaMda	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Deprecated in 10.0, Use {NatIsaMemberSessionUsageHi on nat.IsaMember} instead. The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-275 NatL2AwSubIcmpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubIcmpPortUsageHigh (1086) Type: equipmentAlarm Package: ressubscr.NatL2AwSubIcmpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the ICMP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of the network. If required, deploy extra equipment to deal with the demand.		

Table 19-276 NatL2AwSubSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubSessionUsageHigh (1087) Type: equipmentAlarm Package: ressubscr.NatL2AwSubSessionUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-277 NatL2AwSubTcpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubTcpPortUsageHigh (1088) Type: equipmentAlarm Package: ressubscr.NatL2AwSubTcpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TCP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-278 NatL2AwSubUdpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubUdpPortUsageHigh (1089) Type: equipmentAlarm Package: ressubscr.NatL2AwSubUdpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the UDP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-279 NatLsnSubscriberIcmpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsageHigh (4860) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-280 NatLsnSubscriberIcmpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsgHigh (5397) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-281 NatLsnSubscriberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsageHigh (4861) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 19-282 NatLsnSubscriberSessionUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsgHigh (5398) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 19-283 NatLsnSubscriberTcpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsageHigh (4862) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-284 NatLsnSubscriberTcpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsgHigh (5399) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-285 NatLsnSubscriberUdpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsageHigh (4863) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-286 NatLsnSubscriberUdpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsgHigh (5400) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 19-287 NatMdaDetectsLoadSharingError

Alarm	Attributes	Applicable major release
Name: NatMdaDetectsLoadSharingError (5120) Type: configurationAlarm Package: nat.NatMdaDetectsLoadSharingError Raised on class: nat.IsaMda	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatMdaLoadSharingErrorDetected	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when node is sending periodically at most every 10 seconds while a NAT ISA MDA detects that it is receiving packets erroneously, due to incorrect load-balancing by the ingress IOM. The MDA drops all incorrectly load-balanced traffic.		
Remedial action: The ingress IOM hardware does not support a particular NAT function's load-balancing, for example an IOM-2 does not support deterministic NAT. Upgrade the ingress IOM, or change the configuration.		

Table 19-288 NatPcpSrvStateDown

Alarm	Attributes	Applicable major release
Name: NatPcpSrvStateDown (4382) Type: communicationsAlarm Package: nat.NatPcpSrvStateDown Raised on class: nat.PcpServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatPcpSrvStateDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an NAT PCP Server Changes		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates the PCP Server Operational State is Down.\n Please check the State Description on the PCP server for detail information		

Table 19-289 NatPlL2AwBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlL2AwBlockUsageHigh (1074) Type: equipmentAlarm Package: nat.NatPlL2AwBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the block usage of an L2-aware NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		

Table 19-289 NatPlL2AwBlockUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates the block usage of a L2-aware NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 19-290 NatPlLsnMemberBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlLsnMemberBlockUsageHigh (1075) Type: equipmentAlarm Package: nat.NatPlLsnMemberBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the block usage of a large-scale NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		
Remedial action: This alarm indicates the block usage of a Large Scale NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 19-291 NatResourceProblem

Alarm	Attributes	Applicable major release
Name: NatResourceProblem (9575) Type: equipmentAlarm Package: netw.NatResourceProblem Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: natResourceProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when resource problem is detected while attempting to activate some part of the NAT configuration of a system		
Remedial action: A resource problem was detected while attempting to activate a component of the system NAT configuration. Make sure the ISA card on the NE has sufficient resources available.		

Table 19-292 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-293 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 19-294 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 19-295 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 19-296 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 19-297 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 19-298 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		

Table 19-298 NodeSuspended (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 19-299 noFunctioningScript

Alarm	Attributes	Applicable major release
Name: noFunctioningScript (275) Type: configurationAlarm Package: subscrident.noFunctioningScript Raised on class: subscrident.Policy	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryBackupDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all subscriber identification scripts are operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND ('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR ('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 19-300 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 19-301 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 19-302 NoSFMConfigured

Alarm	Attributes	Applicable major release
Name: NoSFMConfigured (11179) Type: equipmentAlarm Package: netw.NoSFMConfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoSFMConfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when none of the SFM are configured.		
Remedial action: This alarm indicates that none of the SFM is configured. Please configured a SFM.		

Table 19-303 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		

Table 19-303 NTPOperDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 19-304 ObsoleteProtocolInFilter

Alarm	Attributes	Applicable major release
Name: ObsoleteProtocolInFilter (3706) Type: ConfigurationAlarm Package: aapolicy.ObsoleteProtocolInFilter Raised on class: aapolicy.ApplicationFilter	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: obsoleteProtocolInFilter	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a local application filter refers to an obsolete application assurance protocol.		
Remedial action: Change the application filter configuration to use a protocol that is not Obsolete.		

Table 19-305 OesOpticalTrnspndrMiscFailAlarm

Alarm	Attributes	Applicable major release
Name: OesOpticalTrnspndrMiscFailAlarm (11110) Type: equipmentAlarm Package: equipment. OesOpticalTrnspndrMiscFailAlarm Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: opticalTrnspndrMiscFail	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a non-service affecting hardware defect was detected on the card.		
Remedial action: The OesOptTrnspndrMiscFail alarm indicates a lower priority fault on the card that does not directly affect the traffic currently flowing through the card. However, the card should be replaced at the next available maintenance opportunity.		

Table 19-306 OesRedundancyFail

Alarm	Attributes	Applicable major release
Name: OesRedundancyFail (11111) Type: equipmentAlarm Package: equipment.OesRedundancyFail Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RedundancyFail	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when when the inactive equipment controller card in the OES is not providing redundancy protection.		
Remedial action: Check for the Redundancy demerit in the detailed information of the chassis indicated.		

Table 19-307 OFFlowEntryDeploymentCreateFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentCreateFailed (5405) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentCreateFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentCreateFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Creation Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Creation Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects creation of the flow.		

Table 19-308 OFFlowEntryDeploymentDeleteFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentDeleteFailed (5406) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentDeleteFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentDeleteFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Deletion Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Deletion Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects deletion of the flow.		

Table 19-309 OFLogicalPortStatusMplsTpNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusMplsTpNotSet (5407) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusMplsTpNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusMplsTp-NotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the MPLS-TP flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'rsvp-te'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'rsvp-te'))		
Remedial action: When MPLS-TP is not set, OpenFlow port status will not be received by SAM.		

Table 19-310 OFLogicalPortStatusRsvpTeNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusRsvpTeNotSet (5408) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusRsvpTeNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusRs-vpTeNotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RSVP-TE flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'mpls-tp'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'mpls-tp'))		
Remedial action: When RSVP-TE is not set, OpenFlow port status will not be received by SAM.		

Table 19-311 OFSwitchDown

Alarm	Attributes	Applicable major release
Name: OFSwitchDown (5409) Type: equipmentAlarm Package: openflow.OFSwitchDown Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFSwitchDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an OFSwitch is Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is raised when the OpenFlow switch has gone down.		

Table 19-312 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-313 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 19-314 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 19-315 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 19-316 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 19-317 PccRuleInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: PccRuleInsertedFltrEntryDropped (11059) Type: configurationAlarm Package: aclfilter.PccRuleInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a request to insert a filter entry is not successful for a PCC rule application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for PCC rule application. Check the configuration filter entry.		

Table 19-318 PccRuleInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: PccRuleInsertSpaceThresholdAlarm (11058) Type: configurationAlarm Package: aclfilter.PccRuleInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a PCC rule application insert range.		

Table 19-318 PccRuleInsertSpaceThresholdAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for PCC rule application. Make an adjusted to the watermarks or to the filter.		

Table 19-319 PeerConnectionDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: msdp.PeerConnectionDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.		
Raising condition: (('connectionState' NOT EQUAL 'Established') AND ('administrativeState' EQUAL 'Up'))		
Clearing condition: (('connectionState' EQUAL 'Established') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Check the configurations of the peer routers.		

Table 19-320 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 19-321 PeerDown (gmplsuni)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: gmplsuni.PeerDown Raised on class: gmplsuni.Peer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS peer's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS peer's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS peer is down, despite the Administrative state being up. Check if the associated LMP peer or the GMPLS tunnel group endpoint is down.		

Table 19-322 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-323 PeerDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: msdp.PeerDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-323 PeerDown (msdp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('administrativeState' EQUAL 'Down'))		
Clearing condition: (('administrativeState' NOT EQUAL 'Down'))		
Remedial action: Turn up the Peer.		

Table 19-324 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-325 PeerGroupDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: msdp.PeerGroupDown Raised on class: msdp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the Group.		

Table 19-326 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 19-327 PeerUnreachable

Alarm	Attributes	Applicable major release
Name: PeerUnreachable (842) Type: ProtocolAlarm Package: l2tp.PeerUnreachable Raised on class: l2tp.Peer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2TP peer becomes unreachable.		
Remedial action: This alarm is raised when L2TP peer is unreachable. Please verify the L2TP tunnel profile configuration to ensure that the peer is properly configured. Also verify that the peer is actually reachable from this network element. \nThis alarm is cleared automatically when L2TP Peer becomes reachable.		

Table 19-328 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-328 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 19-329 PhysicalLinkPortsMisconfigured

Alarm	Attributes	Applicable major release
Name: PhysicalLinkPortsMisconfigured (239) Type: configurationAlarm Package: netw.PhysicalLinkPortsMisconfigured Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: physicalLinkPortsMisconfig-ured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is an MTU size mismatch between a link endpoint and a port. The alarm clears when the MTUs match.		
Raising condition: ('physicalLinkMisconfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The MTU value(s) on the link endpoint and port must be changed such that they match.		

Table 19-330 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 19-330 PimDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 19-331 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 19-332 PoolDepleted

Alarm	Attributes	Applicable major release
Name: PoolDepleted (3950) Type: configurationAlarm Package: dhcp.PoolDepleted Raised on class: dhcp.AddressPool	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Address pool becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a pool becomes zero. Please increase the pool address range or create another address pool.		

Table 19-333 PoolMinFreeExc

Alarm	Attributes	Applicable major release
Name: PoolMinFreeExc (3696) Type: configurationAlarm Package: dhcp.PoolMinFreeExc Raised on class: dhcp.AddressPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowPoolMin	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		
Remedial action: The alarm is raised when the actual number of free addresses in a pool falls below the desired minimum number specified in the address pool configuration.		

Table 19-334 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol- dExceededAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 19-335 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold- ExceededAlarm	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-335 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 19-336 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-337 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-338 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-339 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-340 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 19-341 PowerSupplyInputFeedDownAlarm

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDownAlarm (5154) Type: equipmentAlarm Package: equipment. PowerSupplyInputFeedDownAlarm Raised on class: equipment.PowerSupply	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 14.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('Input Feed Status' EQUAL 'Input A Down') OR ('Input Feed Status' EQUAL 'Input B Down') OR (('Input Feed Status'allBits'Input A Down') AND ('Input Feed Status'allBits'Input B Down')))		
Clearing condition: ('Input Feed Status' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power		

Table 19-342 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power output fails.		

Table 19-342 PowerSupplyOutputFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-343 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-344 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 19-345 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 19-346 PppoeNcpFailure

Alarm	Attributes	Applicable major release
Name: PppoeNcpFailure (8410) Type: processingErrorAlarm Package: service.PppoeNcpFailure Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapPppoeNcpFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates there is a NCP phase setup problem.		
Remedial action: This alarm indicates the NCP phase setup failed, thus IP protocol can not be configured for the user that attempted to set up the PPPoE session. Please verify NCP setup configuration.		

Table 19-347 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		

Table 19-347 PrimaryImageBootFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 19-348 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 19-349 ProxyMcLocalStateChange

Alarm	Attributes	Applicable major release
Name: ProxyMcLocalStateChange (9039) Type: communicationsAlarm Package: diameter.ProxyMcLocalStateChange Raised on class: diameter.DiameterPeerProxy	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProxyMcLocalStateChange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when proxyMcLocalState of a Diameter Peer Proxy is changed. The states 'active' and 'standby' are normal states.		
Raising condition: (('Local State' NOT EQUAL 'active') OR ('Local State' NOT EQUAL 'standby'))		
Clearing condition: (('Local State' EQUAL 'active') OR ('Local State' EQUAL 'standby'))		
Remedial action: Ensure Proxy multi-chassis redundancy is functionally up.		

Table 19-350 PTPClockNoMasterAlarm

Alarm	Attributes	Applicable major release
Name: PTPClockNoMasterAlarm (3604) Type: communicationsAlarm Package: ptp.PTPClockNoMasterAlarm Raised on class: ptp.IEEEPTPClock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPClockNoMaster	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Precision Timing Protocol (PTP) clock does not support PTP timing master.		
Remedial action: Informational- Please verify master clock configuration for timing.		

Table 19-351 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 19-352 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		

Table 19-352 PTPPeerLossOfAnnounce (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 19-353 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 19-354 PTPPortNoTimestamping

Alarm	Attributes	Applicable major release
Name: PTPPortNoTimestamping (8405) Type: communicationsAlarm Package: ptp.PTPPortNoTimestamping Raised on class: ptp.IEEEPTPPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PerformanceDegraded	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The PtpPortNoTimestamping notification is generated when a PTP port is created and the associated Ethernet port does not support IEEE 1588-2008 port-based timestamping. The PTP port is created but the performance may be degraded due to timestamping at the CPM. For optimal performance, ensure PTP is enabled on ports with IEEE 1588-2008 port-based timestamping capability.		
Remedial action: The Ethernet port used for the PTP port should be changed to a port on an MDA that supports IEEE 1588-2008 port-based timestamping.		

Table 19-355 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 19-356 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 19-357 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-357 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 19-358 PXCAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: PXCAdministrativelyDown (11185) Type: equipmentAlarm Package: pxc.PXCAdministrativelyDown Raised on class: pxc.PortCrossConnect	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portCrossConnectAdministra-tivelyDown	Release: • 14.0
Description: The alarm is raised when the PXC AdministrativelyDown.		
Raising condition: ('Administrative State' EQUAL 'Down')		
Clearing condition: (('Administrative State' EQUAL 'Up'))		
Remedial action: Informational - PortCrossConnect AdministrativelyDown.		

Table 19-359 PXCDown

Alarm	Attributes	Applicable major release
Name: PXCDown (11186) Type: equipmentAlarm Package: pxc.PXCDown Raised on class: pxc.PortCrossConnect	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperablePortCrossConnect	Release: • 14.0
Description: The alarm is raised when the PXC is OperationallyDown.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: This alarm indicates an inoperable PortCrossConnect. Either the associated PhysicalPort or PortCrossConnectSub-ports are down.		

Table 19-360 RadiusAcctPlcyFailure

Alarm	Attributes	Applicable major release
Name: RadiusAcctPlcyFailure (363) Type: radiusAccountingPolicyAlarm Package: radiusaccounting.RadiusAcctPlcyFailure Raised on class: radiusaccounting.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: radiusAccountingRequestFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RADIUS accounting request is not successfully sent to any of the RADIUS servers specified in the RADIUS accounting policy.		
Remedial action: The Radius server(s) which are configured in the accounting policy are unreachable. This may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the Radius server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 19-361 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 19-362 radiusServerOutOfService (subscrauth)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: subscrauth.radiusServerOutOfService Raised on class: subscrauth.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: subAuthPlcyRadSerOperStatChg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-362 radiusServerOutOfService (subscrauth) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the subscriber authentication policy.		

Table 19-363 radiusServerOutOfService (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOutOfService (8406) Type: communicationsAlarm Package: radiusaccounting.radiusServerOutOfService Raised on class: radiusaccounting.RadiusEntry	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radAcctPlcyRadSerOper-StatChg	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RADIUS server is out of service.		
Remedial action: Please verify that:\n(1) RADIUS server is running.\n(2) RADIUS server is properly configured in the RADIUS accounting policy.		

Table 19-364 radiusServerOverloaded (radiusaccounting)

Alarm	Attributes	Applicable major release
Name: radiusServerOverloaded (3913) Type: communicationsAlarm Package: radiusaccounting.radiusServerOverloaded Raised on class: radiusaccounting.RadiusEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusServerRequestLimi-tReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RADIUS server is overloaded.		
Remedial action: Verify the RADIUS server is properly configured to process pending accounting requests at the desired rate and ensure that this rate matches the accounting request limit defined for this RADIUS server on the RADIUS accounting policy.		

Table 19-365 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 19-366 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 19-367 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 19-368 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 19-369 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 19-370 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 19-371 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-372 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 19-373 RPKISessionNotEstablished

Alarm	Attributes	Applicable major release
Name: RPKISessionNotEstablished (8136) Type: communicationsAlarm Package: rtr.RPKISessionNotEstablished Raised on class: rtr.RpkiSession	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RPKISessionNotEstablished	Release: • 12.0 • 13.0 • 14.0

Table 19-373 RPKISessionNotEstablished (continued)

Alarm	Attributes	Applicable major release
Description: The notification alarm is raised when the RPKI Session is not established.		
Raising condition: (('Session State' NOT EQUAL 'Established'))		
Clearing condition: (('Session State' EQUAL 'Established'))		
Remedial action: Make sure that the Cache server is reachable and is configured properly.		

Table 19-374 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 19-375 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 19-376 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 19-377 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 19-378 SapDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosDynamicExceeded (4890) Type: securityServiceOrMechanismViolation Package: service.SapDDosDynamicExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0

Table 19-378 SapDDosDynamicExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the protocol on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpDynamicExcd trap) and the alarm status is set as non-conformant When the SAP starts hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP completes hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 19-379 SapDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosLocMonitorExceeded (4891) Type: securityServiceOrMechanismViolation Package: service.SapDDosLocMonitorExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the SAP (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 19-380 SapDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosStaticExceeded (4892) Type: securityServiceOrMechanismViolation Package: service.SapDDosStaticExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0

Table 19-380 SapDDosStaticExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the static-policer on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpStaticExcd trap) and the alarm status is set as non-conformant. When the SAP starts hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP ends hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 19-381 SapSubAuthError

Alarm	Attributes	Applicable major release
Name: SapSubAuthError (8411) Type: processingErrorAlarm Package: service.SapSubAuthError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 19-382 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 19-383 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 19-384 scriptBackupLost

Alarm	Attributes	Applicable major release
Name: scriptBackupLost (273) Type: configurationAlarm Package: subscrident.scriptBackupLost Raised on class: subscrident.Policy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary subscriber identification script URL is operationally up, but a lower-priority script or URL is operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' EQUAL 'Up') AND (('Secondary Script Operational State' NOT EQUAL 'Up') OR ('Tertiary Script Operational State' NOT EQUAL 'Up')))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' NOT EQUAL 'Up') OR (('Secondary Script Operational State' EQUAL 'Up') AND ('Tertiary Script Operational State' EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 19-385 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 19-386 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 19-387 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 19-388 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 19-389 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-390 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 19-391 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 19-392 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-393 ServerDeclineStaticAddr

Alarm	Attributes	Applicable major release
Name: ServerDeclineStaticAddr (3951) Type: configurationAlarm Package: dhcp.ServerDeclineStaticAddr Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpClientHasStaticIpAddress	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The tmnxDhcpSvrDeclineStaticAddr notification is generated when a DHCP decline message is received from a DHCP client that has a static IP address assigned.		
Remedial action: DHCP client has a static IP address. Make sure that the DHCP client has a dynamic IP address		

Table 19-394 ServerLeaseDefaultTimers

Alarm	Attributes	Applicable major release
Name: ServerLeaseDefaultTimers (2937) Type: configurationAlarm Package: dhcp.ServerLeaseDefaultTimers Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: LeaseTimerInconsistent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the system has reverted to default lease timer values for a particular DHCP client because the configuration of the lease timers was inconsistent.		
Remedial action: This warning is generated when configuration of the lease timers of a particular DHCP client is inconsistent; the system has reverted to default lease timer values. \n The lease renew time T1 and lease rebind time T2 have been reverted to the default value of 1/2 and 2/3 of the lease time.\nPlease check the lease timers configuration on the local DHCP server to ensure the timers are compatible.		

Table 19-395 ServerMaxLeasesReached

Alarm	Attributes	Applicable major release
Name: ServerMaxLeasesReached (3316) Type: configurationAlarm Package: netw.ServerMaxLeasesReached Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMaxLeasesReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the maximum number of leases allocated by local DHCP server is reached.		

Table 19-395 ServerMaxLeasesReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - this alarm indicates that the maximum number of leases allocated by a local DHCP server was reached. The address ranges for existing address pools should be extended or a new address pool should be configured for the local DHCP server.		

Table 19-396 ServerMsgTooLong

Alarm	Attributes	Applicable major release
Name: ServerMsgTooLong (2938) Type: configurationAlarm Package: dhcp.ServerMsgTooLong Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMsgTooLong	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a DHCP message is generated but the message size exceeds either the maximum DHCP message size, or the size provided by the client in the option maximum DHCP message size.		
Remedial action: Review the access network DHCP configuration to ensure all parties send DHCP packets with appropriate message size.		

Table 19-397 ServerUserDatabaseUnknown

Alarm	Attributes	Applicable major release
Name: ServerUserDatabaseUnknown (3952) Type: configurationAlarm Package: dhcp.ServerUserDatabaseUnknown Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CannotFindUserDatabase	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The tmnxDhcpSvrUserDbUnknown notification is generated when the local DHCP server instance drops a DHCP message because a local user database with the name specified for this server instance could not be found.		
Remedial action: Please specify a valid local user database for this server instance.		

Table 19-398 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 19-399 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 19-400 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-401 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 19-402 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment.SonetPathAlarmIndicationSignal Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-403 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-404 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment. SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-405 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-406 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment.SonetPathPayloadMismatch Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 19-407 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 19-408 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment. SonetPathRemoteDefectIndication Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-409 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment. SonetPathUnequippedPathError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-410 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 19-411 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 19-412 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-412 SpbSiteDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 19-413 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 19-414 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 19-415 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 19-416 subHostInconsistentAtmTdOvr

Alarm	Attributes	Applicable major release
Name: subHostInconsistentAtmTdOvr (3685) Type: configurationAlarm Package: ressubscr.subHostInconsistentAtmTdOvr Raised on class: ressubscr.ResidentialSubscriberInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostInconsistentAtmTdOvr	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an AAA server (e.g. a RADIUS server) specifies an ATM Traffic Descriptor override for a subscriber host while it has already specified another one for another host on the same ATM Virtual Circuit.		
Remedial action: Modify the AAA configuration so that all subscriber hosts sharing the same ATM Virtual circuit use the same ATM Traffic Descriptor Override VSA. If different overrides are required, then the subscribers must be in different ATM Virtual Circuits.		

Table 19-417 SubHostLcktLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktLimitReached (4387) Type: configurationAlarm Package: netw.SubHostLcktLimitReached Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the system wide maximum number of lockout hosts is reached.		

Table 19-417 SubHostLcktLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout.		

Table 19-418 SubHostLcktSapLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktSapLimitReached (4391) Type: configurationAlarm Package: service.SubHostLcktSapLimitReached Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktSapLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the maximum number of lockout hosts on a given SAP is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout on the SAP.\n3. Change the Maximum Lockout Hosts (per SAP).		

Table 19-419 SubMcsRelatedProblem

Alarm	Attributes	Applicable major release
Name: SubMcsRelatedProblem (8404) Type: processingErrorAlarm Package: netw.SubMcsRelatedProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subMcsRelatedProblem	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when a subscriber management specific problem occurs during Multi Chassis Syncing, e.g. of DHCP lease states.		
Remedial action: The recovery action depends on the exact cause of the failure. Please review the Additional Text field to obtain information about the specific failure.		

Table 19-420 SubnetDepleted

Alarm	Attributes	Applicable major release
Name: SubnetDepleted (3953) Type: configurationAlarm Package: dhcp.SubnetDepleted Raised on class: dhcp.Subnet	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Subnet becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a subnet becomes zero. Please create another subnet.		

Table 19-421 SubnetMinFreeExc

Alarm	Attributes	Applicable major release
Name: SubnetMinFreeExc (516) Type: configurationAlarm Package: dhcp.SubnetMinFreeExc Raised on class: dhcp.Subnet	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowSubnet-Min	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the actual number of free addresses in a subnet falls below the desired minimum number specified in the subnet configuration		
Remedial action: Please ensure that an adequate free address threshold is configured or create a new subnet to meet the system requirements. \nThis warning is raised on IPv4 DHCP servers only.		

Table 19-422 SubRadSapCoAError

Alarm	Attributes	Applicable major release
Name: SubRadSapCoAError (8416) Type: processingErrorAlarm Package: service.SubRadSapCoAError Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: changeOfAddressError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that system was unable to process a Change of Authorization (CoA) request from a Radius server.		
Remedial action: Please ensure that Accept CoA attribute is properly enabled on the subscriber authentication policy defined for the service. Ensure that the object targeted by the CoA request (a subscriber host for example) is present on the router.		

Table 19-423 SubscriberAuthError (vprn)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: vprn.SubscriberAuthError Raised on class: vprn.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 19-424 SubscriberAuthError (ies)

Alarm	Attributes	Applicable major release
Name: SubscriberAuthError (8387) Type: processingErrorAlarm Package: ies.SubscriberAuthError Raised on class: ies.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subAuthenticationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm indicates that the system encountered a problem while trying to authenticate a subscriber.		
Remedial action: Please review the Additional Text field to obtain information about which subscriber failed the authentication process. Depending on if the subscriber should be allowed or not to access the service, further troubleshooting of the RADIUS server may be required.		

Table 19-425 SubscriberInterfaceDown

Alarm	Attributes	Applicable major release
Name: SubscriberInterfaceDown (440) Type: SubscriberInterfaceAlarm Package: service.SubscriberInterfaceDown Raised on class: service.SubscriberInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a subscriber interface is operationally down. The alarm clears when the subscriber interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		

Table 19-425 SubscriberInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 19-426 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 19-427 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 19-428 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 19-429 SysLicenseExpiresSoon

Alarm	Attributes	Applicable major release
Name: SysLicenseExpiresSoon (9049) Type: equipmentAlarm Package: equipment.SysLicenseExpiresSoon Raised on class: equipment.ProcessorCard	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SystemLicenseExpiresSoon	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the license is due to expire soon.		
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (ASLM).		

Table 19-430 SysLicenseInvalid

Alarm	Attributes	Applicable major release
Name: SysLicenseInvalid (9050) Type: equipmentAlarm Package: equipment.SysLicenseInvalid Raised on class: equipment.ProcessorCard	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SystemLicenseInvalid	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the license becomes invalid for the reason specified in Additional Text.		
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (ASLM).		

Table 19-431 TeLinkDown (gmplsuni)

Alarm	Attributes	Applicable major release
Name: TeLinkDown (8386) Type: ProtocolAlarm Package: gmplsuni.TeLinkDown Raised on class: gmplsuni.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS TE link's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS TE link's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS TE link is down, despite the Administrative state being up. Check if the associated LMP TE link or the GMPLS tunnel group endpoint is down.		

Table 19-432 TeLinkDown (lmp)

Alarm	Attributes	Applicable major release
Name: TeLinkDown (8386) Type: ProtocolAlarm Package: lmp.TeLinkDown Raised on class: lmp.TeLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when a Traffic-Engineering Link has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A network configuration issue has been detected. Ensure the Traffic-Engineering Link configuration between the local node and the peer node is consistent.		

Table 19-433 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		

Table 19-433 TemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 19-434 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 19-435 TMSInterfaceDown

Alarm	Attributes	Applicable major release
Name: TMSInterfaceDown (3907) Type: TMSInterfaceDown Package: service.TMSInterfaceDown Raised on class: service.TmsInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a TMS interface is operationally down. The alarm clears when the TMS interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: This alarm indicates TMS Interface configured is operational down.		

Table 19-436 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 19-437 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 19-438 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 19-439 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 19-439 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 19-440 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 19-441 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 19-442 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 19-443 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-443 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 19-444 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 19-445 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		

Table 19-445 TxSectionSynchronizationError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 19-446 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 19-447 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 19-448 UnrecommendedNAT64DestinationPrefix

Alarm	Attributes	Applicable major release
Name: UnrecommendedNAT64DestinationPrefix (8060) Type: configurationAlarm Package: nat. UnrecommendedNAT64DestinationPrefix Raised on class: nat.Nat64Config	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unrecommendedConfiguration	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the bits [64-71] of NAT64 destination prefix are non-zero for prefix length of 96.		
Raising condition: (('NAT Destination Prefix Length' EQUAL '96') AND ('NAT Destination Prefix' NOT EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Clearing condition: (('NAT Destination Prefix Length' NOT EQUAL '96') OR ('NAT Destination Prefix' EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Remedial action: When using a prefix length 96, set the bits [64-71] of NAT64 Destination Prefix as zero.		

Table 19-449 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 19-450 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 19-451 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 19-452 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0

Table 19-452 UplinkPartiallyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 19-453 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 19-454 VideoInterfaceDown

Alarm	Attributes	Applicable major release
Name: VideoInterfaceDown (794) Type: VideoInterfaceAlarm Package: service.VideoInterfaceDown Raised on class: service.VideoInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a video interface is operationally down. The alarm clears when the video interface is operationally up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 19-455 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-456 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 19-457 VRtrIfDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosDynamicExceeded (4887) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosDynamicExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the protocol on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpDynamicExcd trap) and the alarm status is set as non-conformant When the network interface starts hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface completes hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 19-458 VRtrIfDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosLocMonitorExceeded (4888) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosLocMonitorExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the network interface (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 19-459 VRtrIfDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosStaticExceeded (4889) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosStaticExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the static-policer on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpStaticExcd trap) and the alarm status is set as non-conformant. When the network interface starts hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface ends hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 19-460 WaveTrackerEncoderDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderDegrade (821) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerEncoderDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderDegrade	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade')))		
Remedial action: The OT or SVAC card has detected a DSP failure and this means that the wavelength tracker encode power control is compromised. If this occurs during steady state operation, there is a high probability that the services carried by this OT or SVAC are unaffected. To clear this alarm, replace the card. The card replacement procedure is service affecting and should be conducted during a maintenance window.		

Table 19-461 WaveTrackerEncoderFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderFailure (822) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerEncoderFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure')))		
Remedial action: A cold reset, reseat, or replacement of a card is service impacting if the card is currently carrying services. If there are services currently carried over the card, it may be best to wait for a maintenance window before resetting, replacing, or reseating the card.Confirm that replacement OT or SVAC card supports the same band as the alarmed OT or SVAC card and connect all fibers to the replacement OT or SVAC card.		

Table 19-462 WaveTrackerMissingPluggableVOA

Alarm	Attributes	Applicable major release
Name: WaveTrackerMissingPluggableVOA (4618) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerMissingPluggableVOA Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingPluggableVOA	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA')))		
Remedial action: Informational - no corrective action required.		

Table 19-463 WaveTrackerPowerControlDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlDegrade (823) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlDegrade	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade')))		
Remedial action: check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.		

Table 19-464 WaveTrackerPowerControlFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlFailure (824) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlFailure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure')))		
Remedial action: Either alarmed card has detected equipment problem or there is misfibering problem such that a light-emitting fiber has been plugged into the Tx port of aWavelength Tracker encoder-equipped transponder card.If the card is a transponder card that is equipped with aWavelength Tracker encoder, check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.the card is an SVAC, or if there is no fibering problem on the transponder card.Disconnect all fibers on the alarmed card and Replace the card. connect all fibers to the replacement card		

Table 19-465 WaveTrackerPowerControlHighlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlHighlimit (825) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlHighlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlHighlimit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 19-466 WaveTrackerPowerControllowlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControllowlimit (826) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControllowlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControllowlimit	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control low limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 19-467 WlanGwIsaGrpDegraded

Alarm	Attributes	Applicable major release
Name: WlanGwIsaGrpDegraded (8150) Type: equipmentAlarm Package: wlangw.WlanGwIsaGrpDegraded Raised on class: wlangw.WlanGwIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WlanGwIsaGrpDegraded	Release: • 12.0 • 13.0 • 14.0

Table 19-467 WlanGwIsaGrpDegraded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the WLAN GW ISA group is degraded, while operationally still in service.		
Raising condition: (('Degraded State' EQUAL 'True') AND ('Operational State' EQUAL 'Up'))		
Clearing condition: (('Operational State' NOT EQUAL 'Up') OR ('Degraded State' NOT EQUAL 'True'))		
Remedial action: The ISA-WLAN GW Group is degraded. This alarm occurs when the number of active IOMs in the ISA Group fall below the "Active IOM Limit" configured on the ISA Group. Check the assigned IOM and MDA card statuses.		

Table 19-468 WlanGwIsaGrpDown

Alarm	Attributes	Applicable major release
Name: WlanGwIsaGrpDown (3914) Type: equipmentAlarm Package: wlangw.WlanGwIsaGrpDown Raised on class: wlangw.WlanGwIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WlanGwIsaGrpDown	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an WLAN GW ISA group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-WLAN GW Group is down, despite the administrative state being up. Check that the configured ISA-WLAN GW Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application WLAN GW Group.		

Table 19-469 WlanGwResrcProblemDetected

Alarm	Attributes	Applicable major release
Name: WlanGwResrcProblemDetected (3889) Type: resourceAlarm Package: netw.WlanGwResrcProblemDetected Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is a resource problem detected while attempting to activate some part of the WLAN Gateway configuration of this system.		
Remedial action: The alarm is raised when there is a resource problem detected while attempting to activate some part of the WLAN Gateway configuration of this system.		

Table 19-470 WlanGwTuQosProblem

Alarm	Attributes	Applicable major release
Name: WlanGwTuQosProblem (3915) Type: resourceAlarm Package: wlangw.WlanGwTuQosProblem Raised on class: wlangw.IsaMember	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a resource issue occurs while creating a WLAN Gateway tunnel QoS infrastructure instance.		
Remedial action: This may be a temporary phenomenon. If it persists, the QoS configuration or the scaling may have to be modified to ensure enough resources are available for the UE QoS.		

Table 19-471 WppHostAuthenticationFailed

Alarm	Attributes	Applicable major release
Name: WppHostAuthenticationFailed (3916) Type: processingErrorAlarm Package: wpp.WppHostAuthenticationFailed Raised on class: wpp.Portal	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: portalWppHostAuthentication-Failure	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a WPP host cannot be authenticated.		
Remedial action: The recovery action will depend on the exact failure cause as given by the failureReason.		

Table 19-472 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 19-473 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 10.0 • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

20 7750 SR MG

20.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 20-1 AaPolicerResourcesExceeded

Alarm	Attributes	Applicable major release
Name: AaPolicerResourcesExceeded (2930) Type: configurationAlarm Package: aapolicy.AaPolicerResourcesExceeded Raised on class: aapolicy.AaSubOvrd	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AaPolicerResourcesExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when Application Assurance configured override values exceed policer resources.		
Raising condition: (('Policer Resource Status' EQUAL 'Exceeded'))		
Clearing condition: (('Policer Resource Status' NOT EQUAL 'Exceeded'))		
Remedial action: The Application Assurance Subscriber Policy override(s) configuration has exceeded the policer resources. Remove overrides of a policy configuration for an Application Assurance subscriber where this may be occurring. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-2 AarpDown

Alarm	Attributes	Applicable major release
Name: AarpDown (3704) Type: AarpDown Package: aapolicy.AarpDown Raised on class: aapolicy.Aarp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aarpDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an AARP is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The application assurance redundancy protocol is down either because it is administratively disabled, faulty or a peer address is not up. Ensure that the AARP is administratively up, and the peer ip address and this ip address points to each other.		

Table 20-3 AarpInterfaceDown

Alarm	Attributes	Applicable major release
Name: AarpInterfaceDown (3904) Type: AarpInterfaceDown Package: service.AarpInterfaceDown Raised on class: service.AarpInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an AARP interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 20-4 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 20-5 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 20-5 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 20-6 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 20-7 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 20-8 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 20-9 AGWGTPPMIPPeerDown

Alarm	Attributes	Applicable major release
Name: AGWGTPPMIPPeerDown (1120) Type: EpcAlarm Package: lte.AGWGTPPMIPPeerDown Raised on class: lte.AGWGTPPMIPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AGWGTPPMIPPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the pathManagementState of this EPS peer is not Up.		
Raising condition: ('Path Management State' EQUAL 'Fault')		
Clearing condition: ('Path Management State' EQUAL 'Up')		
Remedial action: A GTP/PMIP based reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 20-10 AGWGTPPMIPPeerLastRestartInfo

Alarm	Attributes	Applicable major release
Name: AGWGTPPMIPPeerLastRestartInfo (5189) Type: EpcAlarm Package: lte.AGWGTPPMIPPeerLastRestartInfo Raised on class: lte.AGWGTPPMIPPeer	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AGWGTPPMIPPeerRestart	Release: • 6.0
Description: The alarm is raised when the pathManagementState of this EPS path is restart and have restart reason and counters information.		
Remedial action: Informational - This alarm give you Peer restart reason and counters information.		

Table 20-11 AGWGTPPMIPPeerRestart

Alarm	Attributes	Applicable major release
Name: AGWGTPPMIPPeerRestart (4415) Type: EpcAlarm Package: lte.AGWGTPPMIPPeerRestart Raised on class: lte.AGWGTPPMIPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AGWGTPPMIPPeerRestart	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the pathManagementState of this EPS path is restart.		
Raising condition: ('Path Management State' EQUAL 'Restart')		
Clearing condition: ('Path Management State' NOT EQUAL 'Restart')		
Remedial action: A path restart is triggered on GTP/PMIP based peer for various reasons: Card reset, or transport issues between MME and SGW, check that the card is operational and check that the underlying transport network is up.		

Table 20-12 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 20-13 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		

Table 20-13 AreaTypeMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 20-14 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 20-15 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 20-16 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 20-17 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 20-18 backupScriptInUse

Alarm	Attributes	Applicable major release
Name: backupScriptInUse (274) Type: configurationAlarm Package: subscrident.backupScriptInUse Raised on class: subscrident.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupInUse	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the primary subscriber identification script is operationally down, but one of the other scripts is operationally up.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND (('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		

Table 20-18 backupScriptInUse (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR (('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 20-19 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 20-20 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 20-21 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 20-22 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 20-23 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 20-24 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 20-25 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-26 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 20-27 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 20-28 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 20-29 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 20-30 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 20-31 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 20-32 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 20-33 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 20-34 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 20-35 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 20-35 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 20-36 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 20-37 BundleDown

Alarm	Attributes	Applicable major release
Name: BundleDown (152) Type: equipmentAlarm Package: bundle.BundleDown Raised on class: bundle.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bundleDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the bundle Administrative State is Up and the Operational State is Down.		
Raising condition: (('Protection Type' EQUAL 'None') AND ('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up') AND ('specificCardType' NOT EQUAL 'Unsupported ASAP Card'))		
Clearing condition: (('Protection Type' NOT EQUAL 'None') OR ('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 20-38 CcagDown

Alarm	Attributes	Applicable major release
Name: CcagDown (210) Type: equipmentAlarm Package: ccag.CcagDown Raised on class: ccag.CrossConnectAggregationGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CcagDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the CCAG Administrative State is Up and the Operational State is Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Informational - no corrective action required.		

Table 20-39 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-40 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-41 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-42 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-43 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-44 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-45 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-46 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 20-47 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 20-48 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 20-49 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 20-50 CoherentOpticalModuleFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleFault (4612) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleFault Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ModuleFault	Release: • 7.0 • 8.0
Description: The alarm is raised when a device reports module fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault')))		
Remedial action: Module Fault occurred.		

Table 20-51 CoherentOpticalModuleHostTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleHostTxFault (4613) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleHostTxFault Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleHostTxFault	Release: • 7.0 • 8.0
Description: The alarm is raised when a device reports Host Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit')))		
Remedial action: Module Host Tx Fault occurred.		

Table 20-52 CoherentOpticalModuleReferenceLockLoss

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleReferenceLockLoss (4614) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleReferenceLockLoss Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceLockLoss	Release: • 7.0 • 8.0
Description: The alarm is raised when a device reports loss of reference lock signal on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module'))		

Table 20-52 CoherentOpticalModuleReferenceLockLoss (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module')))		
Remedial action: Loss of reference lock.		

Table 20-53 CoherentOpticalModuleRxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleRxFault (4615) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleRxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleRxFault	Release: • 7.0 • 8.0
Description: The alarm is raised when a device reports Rx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive')))		
Remedial action: Module Rx Fault occurred.		

Table 20-54 CoherentOpticalModuleTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleTxFault (4616) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleTxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleTxFault	Release: • 7.0 • 8.0
Description: The alarm is raised when a device reports Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit')))		
Remedial action: Module Tx Fault occurred.		

Table 20-55 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback. ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 20-56 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 20-57 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 20-58 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 20-59 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback. ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 20-60 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 20-61 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 20-62 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 20-63 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 20-64 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 20-65 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 20-66 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		

Table 20-66 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 20-67 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-68 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-69 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-70 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtViolPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-71 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-72 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 20-73 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 20-74 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec. CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		

Table 20-74 CpmProtectionViolationVdoVrtrClientEntry (continued)

Alarm	Attributes	Applicable major release
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 20-75 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-76 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-77 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		

Table 20-77 DDMAux1LowAlarm (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-78 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-79 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-80 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 7.0 • 8.0

Table 20-80 DDMAux2HighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-81 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-82 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-83 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-84 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-85 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-86 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-87 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-88 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-89 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-90 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-91 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-92 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-93 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-94 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-95 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-96 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-97 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-98 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-99 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-100 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-101 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 7.0 • 8.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-102 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 7.0 • 8.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 20-103 DeterministicNatMapOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatMapOperDown (9570) Type: equipmentAlarm Package: nat.DeterministicNatMapOperDown Raised on class: nat.DeterministicNatMap	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatMapOper-Down	Release: • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Map is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 20-104 DeterministicNatPrefixOperDown

Alarm	Attributes	Applicable major release
Name: DeterministicNatPrefixOperDown (9571) Type: equipmentAlarm Package: nat.DeterministicNatPrefixOperDown Raised on class: nat.DeterministicNatPrefix	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DeterministicNatPrefixOper-Down	Release: • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a Deterministic NAT Prefix is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'InService') AND ('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: Please verify the configuration.		

Table 20-105 Df2PeerDown

Alarm	Attributes	Applicable major release
Name: Df2PeerDown (4798) Type: EpcLIAlarm Package: lteli.Df2PeerDown Raised on class: lteli.DFPeerCardGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Df2PeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised on a Delivery Function 2 that is operationally down.		
Raising condition: ('DF2 Operational State' NOT EQUAL 'In Service')		
Clearing condition: ('DF2 Operational State' EQUAL 'In Service')		
Remedial action: A TCP connection failure associated with a Delivery Function 2 has occurred. The underlying transport network is unreliable. Please correct the issue within the transport network.		

Table 20-106 Df3PeerDown

Alarm	Attributes	Applicable major release
Name: Df3PeerDown (4799) Type: EpcLIAlarm Package: lteli.Df3PeerDown Raised on class: lteli.DFPeerCardGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Df3PeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised on a Delivery Function 3 that is operationally down.		
Raising condition: ('DF3 Operational State' NOT EQUAL 'In Service')		
Clearing condition: ('DF3 Operational State' EQUAL 'In Service')		
Remedial action: A TCP connection failure associated with a Delivery Function 3 has occurred. The underlying transport network is unreliable. Please correct the issue within the transport network.		

Table 20-107 DHCPPeerDown

Alarm	Attributes	Applicable major release
Name: DHCPPeerDown (5040) Type: EpcAlarm Package: ltegw.DHCPPeerDown Raised on class: ltegw.PdnDhcpSGPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a DHCP peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Up')		
Clearing condition: ('Path Management State' EQUAL 'Up')		
Remedial action: A DHCP server group (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 20-108 DHCPPoolFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPPoolFailoverStateChange (5168) Type: configurationAlarm Package: dhcp.DHCPPoolFailoverStateChange Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPPoolFailoverStateChanged	Release: • 7.0 • 8.0
Description: The alarm is raised when the Local DHCP Pool Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when the operational state of a particular Local DHCP Pool Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a pool failover is in progress.\nThis alarm is cleared implicitly when the DHCP Pool Failover state returns to Normal.		

Table 20-109 DHCPServerFailoverStateChange

Alarm	Attributes	Applicable major release
Name: DHCPServerFailoverStateChange (4986) Type: configurationAlarm Package: dhcp.DHCPServerFailoverStateChange Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DHCPServerFailoverStateChanged	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Local DHCP Server Failover has a state other than Normal.		
Raising condition: (('state' NOT EQUAL 'Normal'))		

Table 20-109 DHCPServerFailoverStateChange (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('state' EQUAL 'Normal'))		
Remedial action: This alarm is raised when operational state of a particular Local DHCP Server Failover is other than Normal.\nThis can occur if the failover configuration is incorrect, disabled or if a server failover is in progress.\nThis alarm will be cleared implicitly when the DHCP Server Failover state returns to Normal.		

Table 20-110 DHCPSFoLeaseUpdateFailedAddressConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedAddressConflict (4977) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedAddressConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedAddressConflict	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a address conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased another address to this host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased another address to this host. Please ensure all configuration is correct.		

Table 20-111 DHCPSFoLeaseUpdateFailedfoShutdown

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedfoShutdown (4985) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedfoShutdown Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedfoShutdown	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a shutdown lease update received from the failover peer cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover state of this DHCP Server instance is 'shutdown'. Please ensure all configuration is correct.		

Table 20-112 DHCPSFoLeaseUpdateFailedHostConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedHostConflict (4978) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedHostConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedHostConflict	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a host conflict lease update received from the failover peer cannot be processed successfully. This DHCP server instance has already leased this address to another host.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. This DHCP server instance has already leased this address to another host. Please ensure all configuration is correct.		

Table 20-113 DHCPSFoLeaseUpdateFailedLeaseExpired

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedLeaseExpired (4979) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedLeaseExpired Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedLeaseExpired	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a lease expired lease update received from the failover peer cannot be processed successfully. The lease received from the peer has expired.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer has expired. Please ensure all configuration is correct.		

Table 20-114 DHCPSFoLeaseUpdateFailedMaxLeaseReached

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedMax-LeaseReached (4980) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedMaxLeaseReached Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedMaxLeaseReached	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a maximum reached lease update received from the failover peer cannot be processed successfully. The maximum number of leases is already reached.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The maximum number of leases is already reached. Please ensure all configuration is correct.		

Table 20-115 DHCPSFoLeaseUpdateFailedPeerConflict

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPeerConflict (4981) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPeerConflict Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPeerConflict	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a peer conflict lease update received from the failover peer cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP server instance. Please ensure all configuration is correct.		

Table 20-116 DHCPSFoLeaseUpdateFailedPersistenceCongested

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedPer-sistenceCongested (4982) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedPersistenceCongested Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedPersistenceCongested	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a persistence congested lease update received from the failover peer cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload. Please ensure all configuration is correct.		

Table 20-117 DHCPSFoLeaseUpdateFailedRangeNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedRangeNotFound (4983) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedRangeNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdateFaile-dRangeNotFound	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a range not found lease update received from the failover peer cannot be processed successfully. No valid include range for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid include range for this lease could be found. Please ensure all configuration is correct.		

Table 20-118 DHCPSFoLeaseUpdateFailedSubnetNotFound

Alarm	Attributes	Applicable major release
Name: DHCPSFoLeaseUpdateFailedSubnetNotFound (4984) Type: configurationAlarm Package: dhcp. DHCPSFoLeaseUpdateFailedSubnetNotFound Raised on class: dhcp.LocalDhcpServerFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPSFoLeaseUpdate-FailedSubnetNotFound	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when a subnet not found lease update received from the failover peer cannot be processed successfully. No valid subnet for this lease could be found.		
Remedial action: This alarm indicates the Local DHCP Server Failover lease update has failed. Packet received from the failover peer, cannot be processed successfully. No valid subnet for this lease could be found. Please ensure all configuration is correct.		

Table 20-119 DiamAppMessageDropped

Alarm	Attributes	Applicable major release
Name: DiamAppMessageDropped (5175) Type: processingErrorAlarm Package: diameter.DiamAppMessageDropped Raised on class: diameter.DiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamAppMessageDropped	Release: • 7.0
Description: The alarm is raised when the Diameter protocol has dropped a message		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 20-120 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 20-121 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 20-122 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 20-123 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 20-124 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 20-125 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment.DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 20-126 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		

Table 20-126 DS1E1SignalDegradation (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational only.		

Table 20-127 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 20-128 DS3E3AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS3E3AlarmIndicationSignal (115) Type: communicationsAlarm Package: tdmequipment.DS3E3AlarmIndicationSignal Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 20-129 DS3E3Looped

Alarm	Attributes	Applicable major release
Name: DS3E3Looped (120) Type: communicationsAlarm Package: tdmequipment.DS3E3Looped Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a remote loopback alarm condition.		

Table 20-129 DS3E3Looped (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 20-130 DS3E3LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS3E3LossOfSignal (116) Type: communicationsAlarm Package: tdmequipment.DS3E3LossOfSignal Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 20-131 DS3E3OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS3E3OutOfFrame (117) Type: communicationsAlarm Package: tdmequipment.DS3E3OutOfFrame Raised on class: tdmequipment. DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 20-132 DS3E3ResourceAvailability

Alarm	Attributes	Applicable major release
Name: DS3E3ResourceAvailability (119) Type: communicationsAlarm Package: tdmequipment.DS3E3ResourceAvailability Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 20-133 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 20-134 EpcDown

Alarm	Attributes	Applicable major release
Name: EpcDown (743) Type: EpcAlarm Package: lte.EpcDown Raised on class: lte.EPCGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an EPC instance is operationally down but administratively up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		

Table 20-134 EpcDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is an indication that the GW card(s) the EPC instance is running on is operationally down. Ensure that the appropriate number of GW card(s) installed in the chassis and are operational.		

Table 20-135 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 20-136 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 20-137 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 20-138 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-139 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when equipment enters a diagnostic state.		

Table 20-139 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 20-140 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 20-141 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 20-142 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 20-143 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 20-144 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		

Table 20-144 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 20-145 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 20-146 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 20-147 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 20-148 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 20-149 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.0 • 7.0 • 8.0

Table 20-149 EthernetPortNoFrameLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 20-150 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 20-151 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 20-152 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 20-153 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 20-154 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 20-155 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 20-156 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 20-157 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		

Table 20-157 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 20-158 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 20-159 GRETunnelDown

Alarm	Attributes	Applicable major release
Name: GRETunnelDown (3326) Type: serviceAlarm Package: svt.GRETunnelDown Raised on class: svt.GRETunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the IP/GRE tunnel Operational State changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The situation may occur if the underlying physical port is down either because of administrative disabling or a fault on the port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable.		

Table 20-160 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 20-161 GroupInterfaceDown

Alarm	Attributes	Applicable major release
Name: GroupInterfaceDown (441) Type: GroupInterfaceAlarm Package: service.GroupInterfaceDown Raised on class: service.GroupInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a group interface is operationally down. The alarm clears when the group interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 20-162 GwCdfDownAlarm

Alarm	Attributes	Applicable major release
Name: GwCdfDownAlarm (2956) Type: communicationsAlarm Package: lte.GwCdfDownAlarm Raised on class: lte.RfReferencePoint	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: connectionDown	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwCdfDownAlarm notification is generated when both the primary and the secondary Charging Data Functions (CDFs) are down for active Rf diameter sessions		
Remedial action: The Charging Data Functions (primary and secondary) are down for a Rf reference point. The CDF function appears down for one of the following reasons: the underlying IP or physical interface is down, the far end diameter peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end diameter peer is operational and check that the underlying transport network is up.		

Table 20-163 GwCfCapacityAlarmMajor

Alarm	Attributes	Applicable major release
Name: GwCfCapacityAlarmMajor (2957) Type: equipmentAlarm Package: lte.GwCfCapacityAlarmMajor Raised on class: lte.AGWReferencePoint	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwCfCapacityAlarmMajor notification is generated when compact flash capacity reaches 95% limit.		
Remedial action: The compact flash device of the MGW is approaching capacity. The contents of the device must be analysed to identify redundant content which can be deleted.		

Table 20-164 GwCfCapacityAlarmMinor

Alarm	Attributes	Applicable major release
Name: GwCfCapacityAlarmMinor (2958) Type: equipmentAlarm Package: lte.GwCfCapacityAlarmMinor Raised on class: lte.AGWReferencePoint	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwCfCapacityAlarmMinor notification is generated when compact flash capacity reaches 85% limit		
Remedial action: The compact flash device of the MGW is approaching capacity. The contents of the device must be analysed to identify redundant content which can be deleted.		

Table 20-165 GwFqdnGrpCamLimitAlarm

Alarm	Attributes	Applicable major release
Name: GwFqdnGrpCamLimitAlarm (8393) Type: EpcAlarm Package: lte.GwFqdnGrpCamLimitAlarm Raised on class: lte.EPCGateway	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Threshold	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwFqdnGrpCamLimitAlarm notification is generated when the CAM resource usage for the DNS resolution of the FQDN group reaches 75% of the CAM resource size. [CAUSE] The CAM resource usage for the DNS resolution of the FQDN group reaches 75% of the CAM resource size because the CAM resource is very close to be exhausted.		
Remedial action: The CAM resource usage for the DNS resolution of the FQDN group reaches 75% of the CAM resource size.Need to look at clearing the resolved filters for the specified FQDN group.		

Table 20-166 GwGtpPriSrvGrpStateChange

Alarm	Attributes	Applicable major release
Name: GwGtpPriSrvGrpStateChange (3635) Type: EpcAlarm Package: lte.GwGtpPriSrvGrpStateChange Raised on class: lte.EPCGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GwGtpPriSrvGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: An alarm is raised when there has been a change in GPRS Tunneling Protocol (GTP) Prime Server state for all mobile system groups.		
Remedial action: If a GTP Prime server group state is down, CDR packets will be written to CDR files until at least one server becomes available.		

Table 20-167 GwMscpUeIdUsgAlarm

Alarm	Attributes	Applicable major release
Name: GwMscpUeIdUsgAlarm (11002) Type: EpcAlarm Package: lte.GwMscpUeIdUsgAlarm Raised on class: lte.EPCGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Threshold	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwMscpUeIdUsgAlarm notification is generated when the User Equipment (UE) ID load count for the MSCP group has crossed the 80% threshold.		
Remedial action: When the User Equipment (UE) ID load count for the MSCP group crosses the 80% threshold, Engage the nokia support team to find out the root cause.		

Table 20-168 GwRadGroupFail

Alarm	Attributes	Applicable major release
Name: GwRadGroupFail (3636) Type: EpcAlarm Package: lte.GwRadGroupFail Raised on class: lte.EPCGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: EPSGroupDown	Release: • 6.0 • 7.0 • 8.0
Description: A tmnxMobGwRadGrpFailAlarm notification is generated when all the radius servers have failed in the radius server group.		
Remedial action: The Radius server(s) which are configured in the Radius Server are unreachable. This problem may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the Radius server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 20-169 GwRadPeerFail

Alarm	Attributes	Applicable major release
Name: GwRadPeerFail (3682) Type: EpcAlarm Package: lteradius.GwRadPeerFail Raised on class: lteradius.PdnRadiusPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: EPSPeerDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM receives a tmnxMobGwRadPeerFailAlarm notification in response to a RADIUS server failure.		
Remedial action: A Radius peer is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 20-170 HostConnectivityLostRateExceeded

Alarm	Attributes	Applicable major release
Name: HostConnectivityLostRateExceeded (276) Type: communicationsAlarm Package: ressubscr. HostConnectivityLostRateExceeded Raised on class: ressubscr.ShcvSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hostDown Applicable probable causes: • hostDown • trapDropped	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the trapDroppedRaisesAlarm parameter is enabled and the maximum allowed number of SHCV host connectivity loss events on a SAP is exceeded. The SHCV action in response to the alarm is specified by the maxHostLostConnectivityRate parameter. If the specified action is to remove the host information, the host information is removed and the connectivity of the host is not subsequently verified.		
Remedial action: This may be a transient error condition in the network or possible congestion or could be a sign that the SHCV ping interval is too short. Verify the status of the network for those subscribers and the service SHCV configuration.		

Table 20-171 IGHMisconfigured

Alarm	Attributes	Applicable major release
Name: IGHMisconfigured (827) Type: ighAlarm Package: igh.IGHMisconfigured Raised on class: igh.InterfaceGroupHandler	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IGHProtocolMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the IGH is administratively up but none of the IGH protocols is operationally up.		
Raising condition: (('igh_misconfigured' EQUAL '\"yes\"') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('igh_misconfigured' NOT EQUAL '\"yes\"') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 20-171 IGHMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please check the configuration.		

Table 20-172 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 20-173 IgmpMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxGrpSrcsLimitExceeded (4624) Type: configurationAlarm Package: igmp.IgmpMaxGrpSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxGrpSrcsLimitExceeded	Release: • 7.0
Description: The alarm is raised when an attempt is made to configure an IGMP group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Needs to increase 'maxGrpSources' value to allow more sources on this interface.		

Table 20-174 IgmpMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxSrcsLimitExceeded (3742) Type: configurationAlarm Package: igmp.IgmpMaxSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxSrcsLimitExceeded	Release: • 7.0
Description: The alarm is raised when an attempt is made to configure an IGMP source for a group when the number of sources for this group is equal to 'maxSources', the maximum number of sources per group supported on the interface.		
Remedial action: Needs to increase 'maxSources' value to allow more sources on this interface.		

Table 20-175 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 20-176 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 20-177 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		

Table 20-177 IncorrectEndPointPeerConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 20-178 IncorrectNeighborConfig

Alarm	Attributes	Applicable major release
Name: IncorrectNeighborConfig (609) Type: configurationAlarm Package: aps.IncorrectNeighborConfig Raised on class: aps.ApsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incorrectNeighborConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the peer does not exist or the neighbor address does not point to a network interface on the NE that contains the peer object.		
Raising condition: (('Type' EQUAL 'MultiChassis') AND ('Neighbor match' EQUAL 'false'))		
Clearing condition: (('Type' EQUAL 'SingleChassis') OR ('Neighbor match' EQUAL 'true'))		
Remedial action: Make sure a peer exist and the neighbor address points to a network interface on the NE that contains the peer object.		

Table 20-179 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 20-180 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 20-181 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis. PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 20-182 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 20-182 InstanceDown (srrp) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the configuration of the instance		

Table 20-183 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 20-184 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 20-185 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0

Table 20-185 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 20-186 InterfaceDown (service)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: service.InterfaceDown Raised on class: service.RedundantInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a redundant interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 20-187 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 20-188 InterfaceDown (vprn)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vprn.InterfaceDown Raised on class: vprn.IPMirrorInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 20-189 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-190 IOMEventOverflow

Alarm	Attributes	Applicable major release
Name: IOMEventOverflow (5617) Type: equipmentAlarm Package: equipment.IOMEventOverflow Raised on class: equipment.BaseCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMEventOverflow	Release: • 7.0
Description: The alarm is generated when tmnxIomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimitReached occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.		
Remedial action: Informational - The alarm will be cleared when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.		

Table 20-191 IOMResUtilizationLimit

Alarm	Attributes	Applicable major release
Name: IOMResUtilizationLimit (5618) Type: equipmentAlarm Package: equipment.IOMResUtilizationLimit Raised on class: equipment.BaseCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMResHighLimitReached Applicable probable causes: • IOMResHighLimitReached • IOMResExhausted	Release: • 7.0
Description: The alarm is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the value of tmnxIomResourceLimitPct.		
Remedial action: Informational - The alarm will be cleared when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.		

Table 20-192 IPSecGatewayDown

Alarm	Attributes	Applicable major release
Name: IPSecGatewayDown (830) Type: serviceAlarm Package: ipsec.IPSecGatewayDown Raised on class: ipsec.IPSecGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: gatewayDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a SAP IPsec gateway changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 20-193 IPSecIsaGrpDown

Alarm	Attributes	Applicable major release
Name: IPSecIsaGrpDown (3745) Type: equipmentAlarm Package: isa.IPSecIsaGrpDown Raised on class: isa.IPSecIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IPSecIsaGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an ISA IPSec group is Down and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 20-193 IPSecIsaGrpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the ISA-Tunnel Group is down, despite the administrative state being up. Check that the configured ISA-Tunnel Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application IPSec(Tunnel) Group.		

Table 20-194 IPSecTunnelBfdConnectionBroken

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionBroken (831) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionBroken Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 20-195 IPSecTunnelBfdConnectionDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionDown (832) Type: serviceAlarm Package: ipsec.IPSecTunnelBfdConnectionDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 20-196 IPSecTunnelBfdConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelBfdConnectionPeerDetectsDown (833) Type: serviceAlarm Package: ipsec. IPSecTunnelBfdConnectionPeerDetectsDown Raised on class: ipsec.IPSecTunnelBfd	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if the route to the BFD peer exist and is up.		

Table 20-197 IPSecTunnelDown

Alarm	Attributes	Applicable major release
Name: IPSecTunnelDown (834) Type: serviceAlarm Package: ipsec.IPSecTunnelDown Raised on class: ipsec.IPSecTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the IPsec tunnel operational state changes to 'down' and the administrative state is 'up'.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Fix the errors indicated in operational flag.		

Table 20-198 IsaAaGrpDown

Alarm	Attributes	Applicable major release
Name: IsaAaGrpDown (647) Type: equipmentAlarm Package: isa.IsaAaGrpDown Raised on class: isa.AaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an ISA-AA group Operational State is Down, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 20-198 IsaAaGrpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the ISA-AA group is down, despite the administrative state being up. Check that the configured ISA-AA Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Assurance MDA.		

Table 20-199 IsaAaSubUnassigned

Alarm	Attributes	Applicable major release
Name: IsaAaSubUnassigned (836) Type: equipmentAlarm Package: isa.IsaAaSubUnassigned Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaSubUnassigned	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. The unassigned subscriber is treated as specified by the Operation Upon Failure parameter in the AA group. Recovery from this condition requires the removal and recreation of the AA subscriber when sufficient resources are available.		
Raising condition: (('Number of Unassigned ESM Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned SAP Subscribers' NOT EQUAL '0L') OR ('Number of Unassigned Spoke SDP Subscribers' NOT EQUAL '0L'))		
Clearing condition: (('Number of Unassigned ESM Subscribers' EQUAL '0L') AND ('Number of Unassigned SAP Subscribers' EQUAL '0L') AND ('Number of Unassigned Spoke SDP Subscribers' EQUAL '0L'))		
Remedial action: The subscriber cannot be assigned to an ISA-AA MDA in an AA group because of insufficient service queues, a high AA subscriber count, or a high AA subscriber statistics collection rate. Remove and recreate the AA subscriber when sufficient resources are available.		

Table 20-200 IsaLnsGrpDown

Alarm	Attributes	Applicable major release
Name: IsaLnsGrpDown (1119) Type: equipmentAlarm Package: isa.IsaLnsGrpDown Raised on class: isa.LnsGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaLnsGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an ISA-LNS group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is caused by administrative shutdown or equipment failure of the MDA members. Review the status of the underlying ISA MDA group members and ensure they are operational.		

Table 20-201 IsaVideoGrpDown

Alarm	Attributes	Applicable major release
Name: IsaVideoGrpDown (775) Type: equipmentAlarm Package: isa.IsaVideoGrpDown Raised on class: isa.VideoGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaVideoGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an ISA video group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-Video Group is down, despite the administrative state being up. Check that the configured ISA-Video Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application Video Group.		

Table 20-202 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 20-203 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 20-204 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 20-205 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 20-206 L2TPDown

Alarm	Attributes	Applicable major release
Name: L2TPDown (841) Type: ProtocolAlarm Package: l2tp.L2TPDown Raised on class: l2tp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an L2TP site becomes administratively down. The alarm clears when the L2TP site becomes administratively up.		
Raising condition: ('Administrative State' EQUAL 'Down')		
Clearing condition: ('Administrative State' EQUAL 'Up')		

Table 20-206 L2TPDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that the L2TP protocol administrative state is down. It is cleared automatically when L2TP administrative state is up again. Please verify the L2TP configuration. This alarm can be safely suppressed if L2TP is not used.		

Table 20-207 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 20-208 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 20-209 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 20-210 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 20-211 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 20-212 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 20-213 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 20-214 liMirrorLiNatL2awSubOperStateDown

Alarm	Attributes	Applicable major release
Name: liMirrorLiNatL2awSubOperStateDown (9567) Type: equipmentAlarm Package: mirrorli. liMirrorLiNatL2awSubOperStateDown Raised on class: mirrorli.LiNatL2AwareSub	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: liMirrorLiNatL2awSubOperStateDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of the NAT L2 Aware subscriber is Down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		

Table 20-214 liMirrorLiNatL2awSubOperStateDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the ISA MDA reboots successfully, or another ISA MDA takes over, no recovery is required. If more resources become available on the ISA MDA, no recovery is required.		

Table 20-215 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 20-216 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-217 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 20-218 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 20-219 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		

Table 20-219 LocalRncvOperDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 20-220 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 20-221 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 20-222 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 20-223 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 20-224 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 20-225 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 20-226 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 20-227 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 20-228 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 20-229 MaxPdnConnections

Alarm	Attributes	Applicable major release
Name: MaxPdnConnections (4795) Type: EpcAlarm Package: lte.MaxPdnConnections Raised on class: lte.PdnApn	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is generated when the maximum number of Packet Data Network (PDN) connections for this Access Point Name (APN) on the gateway is reached.		
Remedial action: Maximum number of PDN connections for this APN on the gateway is reached.To accept new PDN connections, system has to wait until the number of PDN connections goes below the value of PdnApnMaxPdnConnections.		

Table 20-230 McIPsecPeerTunnelGroupMissing

Alarm	Attributes	Applicable major release
Name: McIPsecPeerTunnelGroupMissing (4815) Type: configurationAlarm Package: multichassis. McIPsecPeerTunnelGroupMissing Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC IPsec tunnel group. This can be either the peer tunnel group is misconfigured or the local peer group ID is not configured.		
Raising condition: ('peerTunnelGroupPointer' EQUAL '\"\"')		
Clearing condition: ('peerTunnelGroupPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC IPsec tunnel group or check the local tunnel group's peer group ID has been configured, or delete this one if it is not used.		

Table 20-231 McIPsecTunnelGroupDown

Alarm	Attributes	Applicable major release
Name: McIPsecTunnelGroupDown (4816) Type: redundancyAlarm Package: multichassis.McIPsecTunnelGroupDown Raised on class: multichassis. McPeerIPSecTunnelGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipsecTunnelGroupDown	Release: • 7.0 • 8.0
Description: The alarm is raised when a MC IPsec tunnel group is operationally down while it is administratively up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check if the physical ISA IPsec Tunnel Group or the associated MDA is operationally down.		

Table 20-232 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 20-233 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		

Table 20-233 MCLagDown (lag) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 20-234 McMobileConfigInfo

Alarm	Attributes	Applicable major release
Name: McMobileConfigInfo (4379) Type: integrityViolation Package: multichassis.McMobileConfigInfo Raised on class: multichassis.MultiChassisPeerMobileGateway	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mismatchPeerSets	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the configuration on the peers are erroneous or if they mismatch		
Raising condition: ('Configuration Mismatch Reason' EQUAL '1')		
Remedial action: Check what caused configuration data between the mobile-gateways mismatch and correct the issue for the geo-redundancy to work.		

Table 20-235 McMobileSwitchOver

Alarm	Attributes	Applicable major release
Name: McMobileSwitchOver (4381) Type: equipmentAlarm Package: multichassis.McMobileSwitchOver Raised on class: multichassis.MultiChassisPeerMobileGateway	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: lossOfRedundancy	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the mobile-gateway participating in geo-redundancy switched over from being a slave to a master or master to a slave		
Raising condition: (('Operational Role' EQUAL '1') OR ('Operational Role' EQUAL '2'))		
Remedial action: Check what caused this switch over and check if the primary mobile-gateway is down.		

Table 20-236 McOmcrStatFailedChanged

Alarm	Attributes	Applicable major release
Name: McOmcrStatFailedChanged (8058) Type: communicationsAlarm Package: multichassis.McOmcrStatFailedChanged Raised on class: multichassis.McOmcrStat	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: McOmcrStatFailedChanged	Release: • 7.0 • 8.0

Table 20-236 McOmcrStatFailedChanged (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the value of the object tmnxMcOmcrStatFailed changes from 'notAct' to any of the other values. The alarm is cleared when the value of the object tmnxMcOmcrStatFailed changes to 'notAct' from any of the other values. A transition from 'notAct' or 'no' to 'yes' means that the traffic of some or all associated client application entries' is being dropped. For example, all traffic from some or all of the IPOE subscriber hosts protected by a failed SRRP instance is dropped by this system. A transition to 'no' means that the system has successfully allocated resources for the traffic of all associated client application entries. A transition to 'notAct' means that this system is not performing the active role anymore for this access protection instance. For example, the value of the object tmnxSrrpOperState has become different from 'master' for the corresponding instance.		
Raising condition: ('Instance Failed' NOT EQUAL 'Not Act')		
Clearing condition: ('Instance Failed' EQUAL 'Not Act')		
Remedial action: There are three recovery actions possible, depending on the reason of the transition of the access protection instance. If it is caused by a problem in the access network, fix that problem, or make additional resources available for this access protection instance. If it is caused by a misconfiguration of this system, correct that, or make additional resources available for this access protection instance.		

Table 20-237 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MC endpoint is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 20-238 MCRedirectThresholdReached (vprn)

Alarm	Attributes	Applicable major release
Name: MCRedirectThresholdReached (8135) Type: communicationsAlarm Package: vprn.MCRedirectThresholdReached Raised on class: vprn.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mCRedirectThreshold-Reached	Release: • 6.0 • 7.0
Description: The alarm is raised when the system detects that the number of monitored packets on the slave node reached high threshold.		
Remedial action: A network configuration issue or a partial network failure has been detected. Diagnose and fix the partial network failure.		

Table 20-239 MCRedirectThresholdReached (rtr)

Alarm	Attributes	Applicable major release
Name: MCRedirectThresholdReached (8135) Type: communicationsAlarm Package: rtr.MCRedirectThresholdReached Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mCRedirectThreshold-Reached	Release: • 6.0 • 7.0
Description: The alarm is raised when the system detects that the number of monitored packets on the slave node reached high threshold.		
Remedial action: A network configuration issue or a partial network failure has been detected. Diagnose and fix the partial network failure.		

Table 20-240 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 20-241 MgGroupDown

Alarm	Attributes	Applicable major release
Name: MgGroupDown (837) Type: MgGroupAlarm Package: isa.MgGroupDown Raised on class: isa.MgIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MgGroupDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MG group goes down.		
Raising condition: ('Group Operational State' EQUAL 'Down')		
Clearing condition: ('Group Operational State' NOT EQUAL 'Down')		
Remedial action: The operational state of the ISA-MG Group is down, despite the administrative state being up. Review the status of the underlying ISA-MG Group Members and ensure they are operational.		

Table 20-242 MigrationCompleted

Alarm	Attributes	Applicable major release
Name: MigrationCompleted (753) Type: migrationComplete Package: equipment.MigrationCompleted Raised on class: equipment.NeCardSwapTask	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationComplete	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a card migration event completes.		
Raising condition: ('Status' EQUAL 'Migration completed')		
Remedial action: Informational - no corrective action required.		

Table 20-243 MigrationFailed

Alarm	Attributes	Applicable major release
Name: MigrationFailed (754) Type: migrationFailure Package: equipment.MigrationFailed Raised on class: equipment.NeCardSwapTask	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: migrationFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a card migration event fails.		
Raising condition: (('Status' EQUAL 'Failed - Latest configuration not available') OR ('Status' EQUAL 'Failed - Unable to migrate configuration') OR ('Status' EQUAL 'Failed - Unable to transfer migrated configuration') OR ('Status' EQUAL 'Failed - Unable to reboot network element'))		
Remedial action: This alarm is raised when a card migration fails. The operation has failed for one of the following reasons - a configuration backup could not be created, the configuration transfer failed or the attempt to reboot the card failed. Please re-attempt the migration. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-244 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 20-245 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 20-246 MldMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxGrpSrcsLimitExceeded (5395) Type: configurationAlarm Package: mld.MldMaxGrpSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxGrpSrcsLimitExceeded	Release: • 7.0
Description: The alarm is raised when an attempt is made to configure an MLD group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Increase the value of the 'Maximum Number of Group Sources' attribute in the parent MLD interface so that the number of active MLD group sources stays under the configured threshold.		

Table 20-247 MldMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldMaxSrcsLimitExceeded (5396) Type: configurationAlarm Package: mld.MldMaxSrcsLimitExceeded Raised on class: mld.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldMaxSrcsLimitExceeded	Release: • 7.0
Description: The alarm is raised when an attempt is made to configure an MLD source for a group when the number of sources for this group is equal to 'maxSources', the Maximum Number of Sources per group supported on the interface.		
Remedial action: Increase 'Maximum Number Of Sources' value to allow more sources on this interface.		

Table 20-248 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 20-249 MobileSiteDown

Alarm	Attributes	Applicable major release
Name: MobileSiteDown (1065) Type: EpcAlarm Package: lteservice.MobileSiteDown Raised on class: lteservice.MobileServiceSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS gateway instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('Evolved Packet System Instance' EQUAL '\"\"')		
Clearing condition: ('Evolved Packet System Instance' NOT EQUAL '\"\"')		
Remedial action: Informational - a topology change due to reconfiguration of the transport network has resulted in deletion of a mobile service site. Regenerate the mobile service site by clicking on the re-calculate button on the mobile service properties form.		

Table 20-250 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 20-250 MplsDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 20-251 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 20-252 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		

Table 20-252 MrpAttrTblSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 20-253 MsdpDown

Alarm	Attributes	Applicable major release
Name: MsdpDown (353) Type: ProtocolAlarm Package: msdp.MsdpDown Raised on class: msdp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the MSDP site.		

Table 20-254 MsgQueueFull

Alarm	Attributes	Applicable major release
Name: MsgQueueFull (10261) Type: EpcAlarm Package: lte.MsgQueueFull Raised on class: lte.AGWDiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MsgQueueFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the diameter message queue utilization reaches 100% %, operator should consider the change of the values for DiameterRateLimProfile::MessageRate, DiameterRateLimProfile::BurstSize or the DiameterRateLimProfile::DelayToler of the diameter rate limit profile.		
Remedial action: If the utilization of the diameter message queue reaches 100%, operator should consider the change of the values for MessageRate, BurstSize or the DelayToler of the diameter rate limit profile.		

Table 20-255 MsgQueueHighThreshold

Alarm	Attributes	Applicable major release
Name: MsgQueueHighThreshold (10262) Type: EpcAlarm Package: lte.MsgQueueHighThreshold Raised on class: lte.AGWDiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MsgQueueHighThreshold	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the diameter message queue utilization reaches the percentage defined by the DiameterRateLimProfile.queThrsHigh, the default value is 80%.		
Remedial action: If the utilization of the diameter message queue reaches 100%,operator should consider the change of the values for MessageRate, BurstSize or the DelayToler of the diameter rate limit profile.		

Table 20-256 MsgQueueLowThreshold

Alarm	Attributes	Applicable major release
Name: MsgQueueLowThreshold (10263) Type: EpcAlarm Package: lte.MsgQueueLowThreshold Raised on class: lte.AGWDiameterPeer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MsgQueueLowThreshold	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the diameter message queue utilization reaches the percentage defined by the DiameterRateLimProfile.queThrsLow, the default value is 30%.		
Remedial action: If the utilization of the diameter message queue reaches 100%, operator should consider the change of the values for MessageRate, BurstSize or the DelayToler of the diameter rate limit profile.		

Table 20-257 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 20-258 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 20-259 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 20-260 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		

Table 20-260 MvrConfiguredProxySapNotExist (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 20-261 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 20-262 NatDeterministicChange

Alarm	Attributes	Applicable major release
Name: NatDeterministicChange (5122) Type: configurationAlarm Package: netw.NatDeterministicChange Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatDeterministicMapChanged	Release: • 7.0
Description: The alarm is raised when something changed in the Deterministic NAT map. Such a change may be caused by a modification of the Deterministic NAT Prefix or the Deterministic NAT Map.		
Remedial action: Managers that rely on the offline representation of the Deterministic NAT map should get an updated copy by saving the Deterministic NAT script.		

Table 20-263 NatIsaGrpDegraded

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDegraded (8059) Type: equipmentAlarm Package: nat.NatIsaGrpDegraded Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDegraded	Release: • 7.0 • 8.0
Description: The alarm is raised when the NAT ISA group is degraded, while operationally still in service.		
Raising condition: (('Degraded State' EQUAL 'True') AND ('Operational State' EQUAL 'Up'))		

Table 20-263 NatIsaGrpDegraded (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'Up') OR ('Degraded State' NOT EQUAL 'True'))		
Remedial action: The ISA-NAT Group is degraded. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 20-264 NatIsaGrpDown

Alarm	Attributes	Applicable major release
Name: NatIsaGrpDown (3887) Type: equipmentAlarm Package: nat.NatIsaGrpDown Raised on class: nat.NatIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatIsaGrpDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an NAT ISA group is Down and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The operational state of the ISA-NAT Group is down, despite the administrative state being up. Check that the configured ISA-NAT Group Member MDA(s) are active and operationally up. There may be a fault with the ISA Application NAT Group.		

Table 20-265 NatIsaMemberSessionUsageHi

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHi (3937) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHi Raised on class: nat.IsaMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-266 NatIsaMemberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatIsaMemberSessionUsageHigh (1070) Type: equipmentAlarm Package: nat.NatIsaMemberSessionUsageHigh Raised on class: nat.IsaMda	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0

Table 20-266 NatIsaMemberSessionUsageHigh (continued)

Alarm	Attributes	Applicable major release
Description: Deprecated in 10.0, Use {NatIsaMemberSessionUsageHi on nat.IsaMember} instead. The alarm is raised when the session usage of an ISA-NAT group member reaches the high watermark. The alarm clears when the session usage reaches the low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-267 NatL2AwSubIcmpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubIcmpPortUsageHigh (1086) Type: equipmentAlarm Package: ressubscr.NatL2AwSubIcmpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the ICMP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of the network. If required, deploy extra equipment to deal with the demand.		

Table 20-268 NatL2AwSubSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubSessionUsageHigh (1087) Type: equipmentAlarm Package: ressubscr.NatL2AwSubSessionUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the session usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-269 NatL2AwSubTcpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubTcpPortUsageHigh (1088) Type: equipmentAlarm Package: ressubscr.NatL2AwSubTcpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the TCP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		

Table 20-269 NatL2AwSubTcpPortUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-270 NatL2AwSubUdpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatL2AwSubUdpPortUsageHigh (1089) Type: equipmentAlarm Package: ressubscr.NatL2AwSubUdpPortUsageHigh Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the UDP port usage of an L2-aware NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-271 NatLsnSubscriberIcmpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsageHigh (4860) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-272 NatLsnSubscriberIcmpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberIcmpPortUsgHigh (5397) Type: thresholdCrossed Package: nat.NatLsnSubscriberIcmpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the ICMP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-273 NatLsnSubscriberSessionUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsageHigh (4861) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 20-274 NatLsnSubscriberSessionUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberSessionUsgHigh (5398) Type: thresholdCrossed Package: nat.NatLsnSubscriberSessionUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the session usage of a large-scale NAT subscriber reaches the high watermark. The alarm will be cleared when the session usage of a large-scale NAT subscriber reaches its low watermark again.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network.		

Table 20-275 NatLsnSubscriberTcpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsageHigh (4862) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-276 NatLsnSubscriberTcpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberTcpPortUsgHigh (5399) Type: thresholdCrossed Package: nat.NatLsnSubscriberTcpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the TCP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-277 NatLsnSubscriberUdpPortUsageHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsageHigh (4863) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsageHigh Raised on class: nat.NatManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-278 NatLsnSubscriberUdpPortUsgHigh

Alarm	Attributes	Applicable major release
Name: NatLsnSubscriberUdpPortUsgHigh (5400) Type: thresholdCrossed Package: nat.NatLsnSubscriberUdpPortUsgHigh Raised on class: nat.NatManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the UDP port usage of a large-scale NAT subscriber reaches the high or low watermark.		
Remedial action: Review the watermarks configuration to make sure it matches the capacity of your network. If required, deploy extra equipment to deal with the demand.		

Table 20-279 NatMdaDetectsLoadSharingError

Alarm	Attributes	Applicable major release
Name: NatMdaDetectsLoadSharingError (5120) Type: configurationAlarm Package: nat.NatMdaDetectsLoadSharingError Raised on class: nat.IsaMda	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NatMdaLoadSharingErrorDetected	Release: • 7.0
Description: The alarm is raised when node is sending periodically at most every 10 seconds while a NAT ISA MDA detects that it is receiving packets erroneously, due to incorrect load-balancing by the ingress IOM. The MDA drops all incorrectly load-balanced traffic.		
Remedial action: The ingress IOM hardware does not support a particular NAT function's load-balancing, for example an IOM-2 does not support deterministic NAT. Upgrade the ingress IOM, or change the configuration.		

Table 20-280 NatPcpSrvStateDown

Alarm	Attributes	Applicable major release
Name: NatPcpSrvStateDown (4382) Type: communicationsAlarm Package: nat.NatPcpSrvStateDown Raised on class: nat.PcpServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NatPcpSrvStateDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an NAT PCP Server Changes		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates the PCP Server Operational State is Down.\n Please check the State Description on the PCP server for detail information		

Table 20-281 NatPlL2AwBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlL2AwBlockUsageHigh (1074) Type: equipmentAlarm Package: nat.NatPlL2AwBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the block usage of an L2-aware NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		
Remedial action: This alarm indicates the block usage of a L2-aware NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 20-282 NatPlLsnMemberBlockUsageHigh

Alarm	Attributes	Applicable major release
Name: NatPlLsnMemberBlockUsageHigh (1075) Type: equipmentAlarm Package: nat.NatPlLsnMemberBlockUsageHigh Raised on class: nat.NatPool	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the block usage of a large-scale NAT address pool reaches the high watermark. The alarm clears when the block usage reaches the low watermark.		
Remedial action: This alarm indicates the block usage of a Large Scale NAT address pool reaches its threshold on a particular member MDA of its ISA group. \nPlease ensure the address pool block usage configuration adequate for the system requirement. \nThis alarm will be cleared automatically once the block usage is below the watermark.		

Table 20-283 NatResourceProblem

Alarm	Attributes	Applicable major release
Name: NatResourceProblem (9575) Type: equipmentAlarm Package: netw.NatResourceProblem Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: natResourceProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when resource problem is detected while attempting to activate some part of the NAT configuration of a system		
Remedial action: A resource problem was detected while attempting to activate a component of the system NAT configuration. Make sure the ISA card on the NE has sufficient resources available.		

Table 20-284 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-285 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.0 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 20-286 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 20-287 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 20-288 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 20-289 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 20-290 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 20-291 noFunctioningScript

Alarm	Attributes	Applicable major release
Name: noFunctioningScript (275) Type: configurationAlarm Package: subscrident.noFunctioningScript Raised on class: subscrident.Policy	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryBackupDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all subscriber identification scripts are operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' NOT EQUAL 'Up') AND ('Secondary Script Operational State' NOT EQUAL 'Up') AND ('Tertiary Script Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' EQUAL 'Up') OR ('Secondary Script Operational State' EQUAL 'Up') OR ('Tertiary Script Operational State' EQUAL 'Up')))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 20-292 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		

Table 20-292 nonDeployedAdjacencyExists (continued)

Alarm	Attributes	Applicable major release
Remedial action: Deploy the changes made to the service.		

Table 20-293 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 20-294 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 20-295 ObsoleteProtocolInFilter

Alarm	Attributes	Applicable major release
Name: ObsoleteProtocolInFilter (3706) Type: ConfigurationAlarm Package: aapolicy.ObsoleteProtocolInFilter Raised on class: aapolicy.ApplicationFilter	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: obsoleteProtocolInFilter	Release: • 6.0
Description: The alarm is raised when a local application filter refers to an obsolete application assurance protocol.		

Table 20-295 ObsoleteProtocolInFilter (continued)

Alarm	Attributes	Applicable major release
Remedial action: Change the application filter configuration to use a protocol that is not Obsolete.		

Table 20-296 OFFlowEntryDeploymentCreateFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentCreateFailed (5405) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentCreateFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentCreateFailed	Release: • 7.0 • 8.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Creation Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Creation Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects creation of the flow.		

Table 20-297 OFFlowEntryDeploymentDeleteFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentDeleteFailed (5406) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentDeleteFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentDeleteFailed	Release: • 7.0 • 8.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Deletion Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Deletion Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects deletion of the flow.		

Table 20-298 OFLogicalPortStatusMplsTpNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusMplsTpNotSet (5407) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusMplsTpNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusMplsTpNotSet	Release: • 7.0 • 8.0
Description: The alarm is raised when the MPLS-TP flag is not set in the Logical Port Status.		

Table 20-298 OFLogicalPortStatusMplsTpNotSet (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'rsvp-te'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'rsvp-te'))		
Remedial action: When MPLS-TP is not set, OpenFlow port status will not be received by SAM.		

Table 20-299 OFLogicalPortStatusRsvpTeNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusRsvpTeNotSet (5408) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusRsvpTeNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusRs-vpTeNotSet	Release: • 7.0 • 8.0
Description: The alarm is raised when the RSVP-TE flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'mpls-tp'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'mpls-tp'))		
Remedial action: When RSVP-TE is not set, OpenFlow port status will not be received by SAM.		

Table 20-300 OFSwitchDown

Alarm	Attributes	Applicable major release
Name: OFSwitchDown (5409) Type: equipmentAlarm Package: openflow.OFSwitchDown Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFSwitchDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the Operational State of an OFSwitch is Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is raised when the OpenFlow switch has gone down.		

Table 20-301 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-302 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 20-303 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		

Table 20-303 P2MPLSPDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 20-304 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 20-305 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 20-306 PccRuleInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: PccRuleInsertedFltrEntryDropped (11059) Type: configurationAlarm Package: aclfilter.PccRuleInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a request to insert a filter entry is not successful for a PCC rule application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for PCC rule application. Check the configuration filter entry.		

Table 20-307 PccRuleInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: PccRuleInsertSpaceThresholdAlarm (11058) Type: configurationAlarm Package: aclfilter.PccRuleInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a PCC rule application insert range.		
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for PCC rule application. Make an adjusted to the watermarks or to the filter.		

Table 20-308 PeerConnectionDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: msdp.PeerConnectionDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.		
Raising condition: (('connectionState' NOT EQUAL 'Established') AND ('administrativeState' EQUAL 'Up'))		
Clearing condition: (('connectionState' EQUAL 'Established') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Check the configurations of the peer routers.		

Table 20-309 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 20-310 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-311 PeerDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: msdp.PeerDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('administrativeState' EQUAL 'Down'))		

Table 20-311 PeerDown (msdp) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('administrativeState' NOT EQUAL 'Down'))		
Remedial action: Turn up the Peer.		

Table 20-312 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-313 PeerGroupDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: msdp.PeerGroupDown Raised on class: msdp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the Group.		

Table 20-314 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 20-315 PeerUnreachable

Alarm	Attributes	Applicable major release
Name: PeerUnreachable (842) Type: ProtocolAlarm Package: l2tp.PeerUnreachable Raised on class: l2tp.Peer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an L2TP peer becomes unreachable.		
Remedial action: This alarm is raised when L2TP peer is unreachable. Please verify the L2TP tunnel profile configuration to ensure that the peer is properly configured. Also verify that the peer is actually reachable from this network element. \nThis alarm is cleared automatically when L2TP Peer becomes reachable.		

Table 20-316 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		

Table 20-316 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 20-317 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 20-318 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 20-319 PoolDepleted

Alarm	Attributes	Applicable major release
Name: PoolDepleted (3950) Type: configurationAlarm Package: dhcp.PoolDepleted Raised on class: dhcp.AddressPool	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Address pool becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a pool becomes zero. Please increase the pool address range or create another address pool.		

Table 20-320 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 20-321 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		

Table 20-321 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 20-322 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-323 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-324 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.0 • 7.0 • 8.0

Table 20-324 PowerSupplyFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-325 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.0 • 7.0 • 8.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-326 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 20-327 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.0 • 7.0 • 8.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-328 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.0 • 7.0 • 8.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-329 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 20-330 PppLoopbackDetected

Alarm	Attributes	Applicable major release
Name: PppLoopbackDetected (362) Type: configurationAlarm Package: ppp.PppLoopbackDetected Raised on class: ppp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PppLoopbackDetected	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the value of tmnxPppLocalMagicNumber is the same as the value of tmnxPppRemoteMagic-Number, which indicates that the link may be looped back.		
Raising condition: (('Local Magic Number' EQUAL 'Remote Magic Number') AND ('Local Magic Number' NOT EQUAL '0L'))		
Clearing condition: (('Local Magic Number' NOT EQUAL 'Remote Magic Number') OR ('Local Magic Number' EQUAL '0L'))		
Remedial action: Informational.		

Table 20-331 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 20-332 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		

Table 20-332 PrimaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 20-333 PTPClockNoMasterAlarm

Alarm	Attributes	Applicable major release
Name: PTPClockNoMasterAlarm (3604) Type: communicationsAlarm Package: ptp.PTPClockNoMasterAlarm Raised on class: ptp.IEEEPTPClock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPClockNoMaster	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when Precision Timing Protocol (PTP) clock does not support PTP timing master.		
Remedial action: Informational- Please verify master clock configuration for timing.		

Table 20-334 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 20-335 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		

Table 20-335 PTPPeerLossOfAnnounce (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 20-336 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 20-337 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 20-338 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 20-339 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 20-340 RadiusAcctPlcyFailure

Alarm	Attributes	Applicable major release
Name: RadiusAcctPlcyFailure (363) Type: radiusAccountingPolicyAlarm Package: radiusaccounting.RadiusAcctPlcyFailure Raised on class: radiusaccounting.Policy	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: radiusAccountingRequestFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a RADIUS accounting request is not successfully sent to any of the RADIUS servers specified in the RADIUS accounting policy.		
Remedial action: The Radius server(s) which are configured in the accounting policy are unreachable. This may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the Radius server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 20-341 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 20-342 RcaAuditAfterNEUpgradeStatus

Alarm	Attributes	Applicable major release
Name: RcaAuditAfterNEUpgradeStatus (5124) Type: configurationAlarm Package: netw.RcaAuditAfterNEUpgradeStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: rcaAuditStatusAfterNEUp-grade	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects an NE software version upgrade and RCA audit performed.		
Remedial action: Information - Check audit results for details		

Table 20-343 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 20-344 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 20-345 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 20-346 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		

Table 20-346 RemoteMepCCMAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 20-347 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 20-348 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 20-349 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-350 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 20-351 RPKISessionNotEstablished

Alarm	Attributes	Applicable major release
Name: RPKISessionNotEstablished (8136) Type: communicationsAlarm Package: rtr.RPKISessionNotEstablished Raised on class: rtr.RpkiSession	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RPKISessionNotEstablished	Release: • 7.0 • 8.0
Description: The notification alarm is raised when the RPKI Session is not established.		
Raising condition: (('Session State' NOT EQUAL 'Established'))		
Clearing condition: (('Session State' EQUAL 'Established'))		

Table 20-351 RPKISessionNotEstablished (continued)

Alarm	Attributes	Applicable major release
Remedial action: Make sure that the Cache server is reachable and is configured properly.		

Table 20-352 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 20-353 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 20-354 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 20-355 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 20-356 SapDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosDynamicExceeded (4890) Type: securityServiceOrMechanismViolation Package: service.SapDDosDynamicExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the protocol on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpDynamicExcd trap) and the alarm status is set as non-conformant When the SAP starts hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP completes hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpDynamicConform trap), the alarm will be cleared.		

Table 20-356 SapDDosDynamicExceeded (continued)

Alarm	Attributes	Applicable major release
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 20-357 SapDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosLocMonitorExceeded (4891) Type: securityServiceOrMechanismViolation Package: service.SapDDosLocMonitorExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the SAP (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 20-358 SapDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosStaticExceeded (4892) Type: securityServiceOrMechanismViolation Package: service.SapDDosStaticExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the static-policer on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpStaticExcd trap) and the alarm status is set as non-conformant. When the SAP starts hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP ends hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 20-359 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 20-360 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 20-361 scriptBackupLost

Alarm	Attributes	Applicable major release
Name: scriptBackupLost (273) Type: configurationAlarm Package: subscrident.scriptBackupLost Raised on class: subscrident.Policy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backupDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the primary subscriber identification script URL is operationally up, but a lower-priority script or URL is operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Primary Script Operational State' EQUAL 'Up') AND (('Secondary Script Operational State' NOT EQUAL 'Up') OR ('Tertiary Script Operational State' NOT EQUAL 'Up')))		

Table 20-361 scriptBackupLost (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('isLocal' EQUAL 'true') AND (('Primary Script Operational State' NOT EQUAL 'Up') OR (('Secondary Script Operational State' EQUAL 'Up') AND ('Tertiary Script Operational State' EQUAL 'Up'))))		
Remedial action: If the DHCP ACK Python script processing behaviour is desired, please make sure that primary, secondary and tertiary scripts are installed and operationally up.		

Table 20-362 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 20-363 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 20-364 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 20-365 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 20-366 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		

Table 20-366 SectionB1Error (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-367 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 20-368 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 20-369 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-370 ServerDeclineStaticAddr

Alarm	Attributes	Applicable major release
Name: ServerDeclineStaticAddr (3951) Type: configurationAlarm Package: dhcp.ServerDeclineStaticAddr Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpClientHasStaticIpAddress	Release: • 6.0 • 7.0 • 8.0
Description: The tmnxDhcpSvrDeclineStaticAddr notification is generated when a DHCP decline message is received from a DHCP client that has a static IP address assigned.		
Remedial action: DHCP client has a static IP address. Make sure that the DHCP client has a dynamic IP address		

Table 20-371 ServerLeaseDefaultTimers

Alarm	Attributes	Applicable major release
Name: ServerLeaseDefaultTimers (2937) Type: configurationAlarm Package: dhcp.ServerLeaseDefaultTimers Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: LeaseTimerInconsistent	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the system has reverted to default lease timer values for a particular DHCP client because the configuration of the lease timers was inconsistent.		
Remedial action: This warning is generated when configuration of the lease timers of a particular DHCP client is inconsistent; the system has reverted to default lease timer values. \n The lease renew time T1 and lease rebind time T2 have been reverted to the default value of 1/2 and 2/3 of the lease time.\nPlease check the lease timers configuration on the local DHCP server to ensure the timers are compatible.		

Table 20-372 ServerMaxLeasesReached

Alarm	Attributes	Applicable major release
Name: ServerMaxLeasesReached (3316) Type: configurationAlarm Package: netw.ServerMaxLeasesReached Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMaxLeasesReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the maximum number of leases allocated by local DHCP server is reached.		
Remedial action: Informational - this alarm indicates that the maximum number of leases allocated by a local DHCP server was reached. The address ranges for existing address pools should be extended or a new address pool should be configured for the local DHCP server.		

Table 20-373 ServerMsgTooLong

Alarm	Attributes	Applicable major release
Name: ServerMsgTooLong (2938) Type: configurationAlarm Package: dhcp.ServerMsgTooLong Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMsgTooLong	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a DHCP message is generated but the message size exceeds either the maximum DHCP message size, or the size provided by the client in the option maximum DHCP message size.		
Remedial action: Review the access network DHCP configuration to ensure all parties send DHCP packets with appropriate message size.		

Table 20-374 ServerUserDatabaseUnknown

Alarm	Attributes	Applicable major release
Name: ServerUserDatabaseUnknown (3952) Type: configurationAlarm Package: dhcp.ServerUserDatabaseUnknown Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CannotFindUserDatabase	Release: • 6.0 • 7.0 • 8.0
Description: The tmnxDhcpSvrUserDbUnknown notification is generated when the local DHCP server instance drops a DHCP message because a local user database with the name specified for this server instance could not be found.		
Remedial action: Please specify a valid local user database for this server instance.		

Table 20-375 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 20-376 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 20-377 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 20-377 ShamLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-378 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 20-379 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-380 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-381 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-382 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		

Table 20-382 SonetPathLossOfPointer (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-383 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment. SonetPathPayloadMismatch Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 20-384 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 20-385 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteDefectIndication Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-386 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment.SonetPathUnequippedPathError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-387 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 7.0 • 8.0

Table 20-387 SpbAdjacencyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 20-388 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0 • 8.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 20-389 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.0 • 8.0
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 20-390 StatsRetrieval

Alarm	Attributes	Applicable major release
Name: StatsRetrieval (8069) Type: equipmentAlarm Package: netw.StatsRetrieval Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapGapExceeded	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects trap Gap Exceeded and MG Stats files are retrieved.		
Remedial action: Informational - no corrective action required.		

Table 20-391 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 20-392 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 20-393 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 20-394 subHostInconsistentAtmTdOvr

Alarm	Attributes	Applicable major release
Name: subHostInconsistentAtmTdOvr (3685) Type: configurationAlarm Package: ressubscr.subHostInconsistentAtmTdOvr Raised on class: ressubscr. ResidentialSubscriberInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostInconsistentAtmTdOvr	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an AAA server (e.g. a RADIUS server) specifies an ATM Traffic Descriptor override for a subscriber host while it has already specified another one for another host on the same ATM Virtual Circuit.		
Remedial action: Modify the AAA configuration so that all subscriber hosts sharing the same ATM Virtual circuit use the same ATM Traffic Descriptor Override VSA. If different overrides are required, then the subscribers must be in different ATM Virtual Circuits.		

Table 20-395 SubHostLcktLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktLimitReached (4387) Type: configurationAlarm Package: netw.SubHostLcktLimitReached Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktLimitReached	Release: • 7.0
Description: This alarm is raised when the system wide maximum number of lockout hosts is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout.		

Table 20-396 SubHostLcktSapLimitReached

Alarm	Attributes	Applicable major release
Name: SubHostLcktSapLimitReached (4391) Type: configurationAlarm Package: service.SubHostLcktSapLimitReached Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxSubHostLcktSapLimitReached	Release: • 7.0
Description: This alarm is raised when the maximum number of lockout hosts on a given SAP is reached.		
Remedial action: Please do one of the following:\n1. Investigate why the hosts are locked out. Possible reasons include authentication failure due to mis-configuration on the host end, mis-configuration on the BNG, missing or invalid configuration on the RADIUS server, session negotiation failure with the client, resource exhaustion on the BNG, unavailability of RADIUS server (and no fallback configured).\n2. Clear the host lockout on the SAP.\n3. Change the Maximum Lockout Hosts (per SAP).		

Table 20-397 SubnetDepleted

Alarm	Attributes	Applicable major release
Name: SubnetDepleted (3953) Type: configurationAlarm Package: dhcp.SubnetDepleted Raised on class: dhcp.Subnet	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrDepleted	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is generated when the actual number of free addresses in the DHCP Server Subnet becomes zero.		
Remedial action: This alarm is generated when the actual number of free addresses in a subnet becomes zero. Please create another subnet.		

Table 20-398 SubnetMinFreeExc

Alarm	Attributes	Applicable major release
Name: SubnetMinFreeExc (516) Type: configurationAlarm Package: dhcp.SubnetMinFreeExc Raised on class: dhcp.Subnet	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: actualFreeAddrBelowSubnetMin	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the actual number of free addresses in a subnet falls below the desired minimum number specified in the subnet configuration		
Remedial action: Please ensure that an adequate free address threshold is configured or create a new subnet to meet the system requirements. \nThis warning is raised on IPv4 DHCP servers only.		

Table 20-399 SubscriberInterfaceDown

Alarm	Attributes	Applicable major release
Name: SubscriberInterfaceDown (440) Type: SubscriberInterfaceAlarm Package: service.SubscriberInterfaceDown Raised on class: service.SubscriberInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a subscriber interface is operationally down. The alarm clears when the subscriber interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 20-400 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 20-401 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		

Table 20-401 SubSysChassMemoryUsageHi (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 20-402 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 20-403 SysLicenseExpiresSoon

Alarm	Attributes	Applicable major release
Name: SysLicenseExpiresSoon (9049) Type: equipmentAlarm Package: equipment.SysLicenseExpiresSoon Raised on class: equipment.ProcessorCard	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SystemLicenseExpiresSoon	Release: • 7.0
Description: The alarm is raised when the license is due to expire soon.		
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (ASLM).		

Table 20-404 SysLicenseInvalid

Alarm	Attributes	Applicable major release
Name: SysLicenseInvalid (9050) Type: equipmentAlarm Package: equipment.SysLicenseInvalid Raised on class: equipment.ProcessorCard	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SystemLicenseInvalid	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the license becomes invalid for the reason specified in Additional Text.		
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (ASLM).		

Table 20-405 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 20-406 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 20-407 TMSInterfaceDown

Alarm	Attributes	Applicable major release
Name: TMSInterfaceDown (3907) Type: TMSInterfaceDown Package: service.TMSInterfaceDown Raised on class: service.TmsInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a TMS interface is operationally down. The alarm clears when the TMS interface is operationally up.		
Raising condition: ('operationalState' NOT EQUAL 'Up')		
Clearing condition: ('operationalState' EQUAL 'Up')		

Table 20-407 TMSInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates TMS Interface configured is operational down.		

Table 20-408 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 20-409 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 7.0 • 8.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 20-410 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 20-411 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.0 • 7.0 • 8.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		

Table 20-411 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 20-412 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.0 • 7.0 • 8.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 20-413 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 20-414 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 20-415 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 20-416 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 20-417 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 20-418 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 20-419 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		

Table 20-419 UnmanageFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 20-420 UnrecommendedNAT64DestinationPrefix

Alarm	Attributes	Applicable major release
Name: UnrecommendedNAT64DestinationPrefix (8060) Type: configurationAlarm Package: nat. UnrecommendedNAT64DestinationPrefix Raised on class: nat.Nat64Config	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unrecommendedConfiguration	Release: • 6.0 • 7.0 • 8.0
Description: This alarm is raised when the bits [64-71] of NAT64 destination prefix are non-zero for prefix length of 96.		
Raising condition: (('NAT Destination Prefix Length' EQUAL '96') AND ('NAT Destination Prefix' NOT EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Clearing condition: (('NAT Destination Prefix Length' NOT EQUAL '96') OR ('NAT Destination Prefix' EQUAL '\"([0-9A-F]{1,4}:){4}([0-9A-F]{1,2})(:[0-9A-F]{1,4}){3}\"'))		
Remedial action: When using a prefix length 96, set the bits [64-71] of NAT64 Destination Prefix as zero.		

Table 20-421 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 20-422 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 20-423 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 20-424 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 20-425 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 20-426 VideoInterfaceDown

Alarm	Attributes	Applicable major release
Name: VideoInterfaceDown (794) Type: VideoInterfaceAlarm Package: service.VideoInterfaceDown Raised on class: service.VideoInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a video interface is operationally down. The alarm clears when the video interface is operationally up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check the configuration and the underlying physical interface.		

Table 20-427 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 20-427 VirtualLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-428 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 20-429 VRtrIfDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosDynamicExceeded (4887) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosDynamicExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the protocol on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpDynamicExcd trap) and the alarm status is set as non-conformant When the network interface starts hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface completes hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 20-430 VRtrIfDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosLocMonitorExceeded (4888) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosLocMonitorExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the network interface (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 20-431 VRtrIfDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosStaticExceeded (4889) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosStaticExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 7.0
Description: The alarm is raised when the static-policer on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpStaticExcd trap) and the alarm status is set as non-conformant. When the network interface starts hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface ends hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 20-432 WaveTrackerEncoderDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderDegrade (821) Type: communicationsAlarm Package: ethernetequipment.WaveTrackerEncoderDegrade Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderDegrade	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports an encoder degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade')))		
Remedial action: The OT or SVAC card has detected a DSP failure and this means that the wavelength tracker encode power control is compromised. If this occurs during steady state operation, there is a high probability that the services carried by this OT or SVAC are unaffected. To clear this alarm, replace the card. The card replacement procedure is service affecting and should be conducted during a maintenance window.		

Table 20-433 WaveTrackerEncoderFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderFailure (822) Type: communicationsAlarm Package: ethernetequipment.WaveTrackerEncoderFailure Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports an encoder failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure')))		
Remedial action: A cold reset, reseat, or replacement of a card is service impacting if the card is currently carrying services. If there are services currently carried over the card, it may be best to wait for a maintenance window before resetting, replacing, or reseating the card.Confirm that replacement OT or SVAC card supports the same band as the alarmed OT or SVAC card and connect all fibers to the replacement OT or SVAC card.		

Table 20-434 WaveTrackerMissingPluggableVOA

Alarm	Attributes	Applicable major release
Name: WaveTrackerMissingPluggableVOA (4618) Type: communicationsAlarm Package: ethernetequipment.WaveTrackerMissingPluggableVOA Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingPluggableVOA	Release: • 6.0 • 7.0 • 8.0

Table 20-434 WaveTrackerMissingPluggableVOA (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA')))		
Remedial action: Informational - no corrective action required.		

Table 20-435 WaveTrackerPowerControlDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlDegrade (823) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlDegrade	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a power control degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade')))		
Remedial action: check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.		

Table 20-436 WaveTrackerPowerControlFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlFailure (824) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlFailure	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a power control failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure')))		

Table 20-436 WaveTrackerPowerControlFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Either alarmed card has detected equipment problem or there is misfibering problem such that a light-emitting fiber has been plugged into the Tx port of aWavelength Tracker encoder-equipped transponder card.If the card is a transponder card that is equipped with aWavelength Tracker encoder, check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.the card is an SVAC, or if there is no fibering problem on the transponder card.Disconnect all fibers on the alarmed card and Replace the card. connect all fibers to the replacement card		

Table 20-437 WaveTrackerPowerControlHighlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlHighlimit (825) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlHighlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlHighlimit	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 20-438 WaveTrackerPowerControllowlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControllowlimit (826) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControllowlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControllowlimit	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when a device reports a power control low limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 20-439 WlanGwResrcProblemDetected

Alarm	Attributes	Applicable major release
Name: WlanGwResrcProblemDetected (3889) Type: resourceAlarm Package: netw.WlanGwResrcProblemDetected Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.0
Description: The alarm is raised when there is a resource problem detected while attempting to activate some part of the WLAN Gateway configuration of this system.		
Remedial action: The alarm is raised when there is a resource problem detected while attempting to activate some part of the WLAN Gateway configuration of this system.		

Table 20-440 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 20-441 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 6.0 • 7.0 • 8.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

21 7950 XRS

21.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 21-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 21-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 21-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 21-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 21-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 21-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 21-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 21-8 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 21-9 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 21-10 AtcaPowerSupplyFailure

Alarm	Attributes	Applicable major release
Name: AtcaPowerSupplyFailure (1125) Type: equipmentAlarm Package: equipment.AtcaPowerSupplyFailure Raised on class: equipment.PowerSupply	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the associated power supply is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled'))		
Clearing condition: ('operationalState' EQUAL 'Enabled')		
Remedial action: Check the status of the site power supply.		

Table 21-11 AuthKeyConflict (rsvp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: rsvp.AuthKeyConflict Raised on class: rsvp.AuthenticationKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when both Authentication Key and RSVP Keychain are configured. RSVP Keychain will be used.		
Raising condition: (('RSVP Keychain' NOT EQUAL '\"\"') AND ('enableAuthentication' EQUAL 'true'))		
Clearing condition: (('RSVP Keychain' EQUAL '\"\"') OR ('enableAuthentication' NOT EQUAL 'true'))		
Remedial action: Authentication Key and RSVP Keychain are both configured. RSVP Keychain will be used. The alarm is cleared when only one is configured.		

Table 21-12 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 21-13 BackPlaneEPROMFailed

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMFailed (12488) Type: equipmentAlarm Package: netw.BackPlaneEPROMFailed Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access the backplane EPROM due to a hardware defect.		
Remedial action: The active CPM is at risk of failing to initialize after node reboot due to not being able to access the BP EPROM to read the chassis type. Contact Nokia customer support.		

Table 21-14 BackPlaneEPROMWarning

Alarm	Attributes	Applicable major release
Name: BackPlaneEPROMWarning (12489) Type: equipmentAlarm Package: netw.BackPlaneEPROMWarning Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the active CPM is no longer able to access one backplane EPROM due to a hardware defect but a redundant EPROM is present and accessible.		
Remedial action: There is no effect on system operation.No recovery action required.		

Table 21-15 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 21-16 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 21-17 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 21-18 BfdInterfaceConnectionBroken

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionBroken (3329) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionBroken Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionBroken	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BFD connection to a peer times out.		
Raising condition: ('Operational State' EQUAL 'Timed Out')		
Clearing condition: ('Operational State' NOT EQUAL 'Timed Out')		
Remedial action: Check the peer router, fix the BFD connection		

Table 21-19 BfdInterfaceConnectionDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionDown (3330) Type: serviceAlarm Package: vrrp.BfdInterfaceConnectionDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of a BFD session is Not Connected.		
Raising condition: ('Operational State' NOT EQUAL 'Operational')		
Clearing condition: ('Operational State' EQUAL 'Operational')		
Remedial action: Check the BFD interface configuration, fix the BFD connection		

Table 21-20 BfdInterfaceConnectionPeerDetectsDown

Alarm	Attributes	Applicable major release
Name: BfdInterfaceConnectionPeerDetectsDown (3331) Type: serviceAlarm Package: vrrp. BfdInterfaceConnectionPeerDetectsDown Raised on class: vrrp.BfdInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionConnectionPeer-DetectsDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BFD peer detects a connection timeout.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Fix the BFD connection		

Table 21-21 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-22 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 21-23 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 21-24 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 21-25 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 21-26 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 21-27 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 21-28 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 21-29 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 21-30 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 21-31 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 21-32 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 21-33 CardDegrade

Alarm	Attributes	Applicable major release
Name: CardDegrade (1987) Type: equipmentAlarm Package: equipment.CardDegrade Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EqptDgr	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Card degrade - device is detected.		
Remedial action: At the end of each step wait to see if the fault clears. If not, continue with the next step.1. Is the alarmed pack a 100G Coherent OT (112SCA1, 112SNA1, 112SCX10 or 112SNX10)? 2. Check the line port information and Line port PM.If the OPT and OPR parameters are blank go to Step 3.3. Check the firmware profile that is currently running on the pack.If not, go to Step 7.If the firmware profile for the card is lower than the versions shown in the table below,then the firmware should be upgraded see - Selecting a Specific Firmware Version 4. Perform a cold reset of the card.5. Reseat the card.6. Replace the card.7. Perform a warm reset of the card.		

Table 21-34 CesBfrOverrun

Alarm	Attributes	Applicable major release
Name: CesBfrOverrun (448) Type: communicationsAlarm Package: vll.CesBfrOverrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer overrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Overrun') AND ('Report Alarm'anyBit'Buffer Overrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-35 CesBfrUnderrun

Alarm	Attributes	Applicable major release
Name: CesBfrUnderrun (449) Type: communicationsAlarm Package: vll.CesBfrUnderrun Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverrun	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a jitter buffer underrun.		
Raising condition: (('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Buffer Underrun') AND ('Report Alarm'anyBit'Buffer Underrun')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-36 CesMalformedPkts

Alarm	Attributes	Applicable major release
Name: CesMalformedPkts (446) Type: communicationsAlarm Package: vll.CesMalformedPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: malformedPackets	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects one or more malformed packets.		
Raising condition: (('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Malformed Packets') AND ('Report Alarm'anyBit'Malformed Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-37 CesPktLoss

Alarm	Attributes	Applicable major release
Name: CesPktLoss (447) Type: communicationsAlarm Package: vll.CesPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPacket	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Packet Loss') AND ('Report Alarm'anyBit'Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-38 CesRmtPktLoss

Alarm	Attributes	Applicable major release
Name: CesRmtPktLoss (450) Type: communicationsAlarm Package: vll.CesRmtPktLoss Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLossOfPacket	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote packet loss.		
Raising condition: (('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote Packet Loss') AND ('Report Alarm'anyBit'Remote Packet Loss')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-39 CesRmtRdi

Alarm	Attributes	Applicable major release
Name: CesRmtRdi (452) Type: configurationAlarm Package: vll.CesRmtRdi Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: farEndRdi	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote RDI.		
Raising condition: (('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote RDI') AND ('Report Alarm'anyBit'Remote RDI')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-40 CesRmtTdmFault

Alarm	Attributes	Applicable major release
Name: CesRmtTdmFault (451) Type: configurationAlarm Package: vll.CesRmtTdmFault Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tdmFarEndFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a remote TDM fault.		
Raising condition: (('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Remote TDM Fault') AND ('Report Alarm'anyBit'Remote TDM Fault')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-41 CesStrayPkts

Alarm	Attributes	Applicable major release
Name: CesStrayPkts (445) Type: communicationsAlarm Package: vll.CesStrayPkts Raised on class: vll.VllCesInterfaceSpecifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: strayPackets	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects received stray packets.		
Raising condition: (('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets'))		
Clearing condition: NOT ((('Report Alarm Status'anyBit'Stray Packets') AND ('Report Alarm'anyBit'Stray Packets')))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 21-42 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 21-43 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 21-44 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 21-45 CoherentOpticalModuleFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleFault (4612) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ModuleFault	Release: • 14.0
Description: The alarm is raised when a device reports module fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module Fault') AND ('Reported Alarms'anyBit'Module Fault')))		
Remedial action: Module Fault occurred.		

Table 21-46 CoherentOpticalModuleHostTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleHostTxFault (4613) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleHostTxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleHostTxFault	Release: • 14.0
Description: The alarm is raised when a device reports Host Tx Fault on a coherent optical interface.		

Table 21-46 CoherentOpticalModuleHostTxFault (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Host (Electrical Side) Transmit') AND ('Reported Alarms'anyBit'Host (Electrical Side) Transmit')))		
Remedial action: Module Host Tx Fault occurred.		

Table 21-47 CoherentOpticalModuleReferenceLockLoss

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleReferenceLockLoss (4614) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleReferenceLockLoss Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceLockLoss	Release: • 14.0
Description: The alarm is raised when a device reports loss of reference lock signal on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Module') AND ('Reported Alarms'anyBit'Module')))		
Remedial action: Loss of reference lock.		

Table 21-48 CoherentOpticalModuleRxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleRxFault (4615) Type: communicationsAlarm Package: ethernetequipment. CoherentOpticalModuleRxFault Raised on class: ethernetequipment. CoherentOpticalCfg	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleRxFault	Release: • 14.0
Description: The alarm is raised when a device reports Rx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Receive') AND ('Reported Alarms'anyBit'Network (Optical Side) Receive')))		
Remedial action: Module Rx Fault occurred.		

Table 21-49 CoherentOpticalModuleTxFault

Alarm	Attributes	Applicable major release
Name: CoherentOpticalModuleTxFault (4616) Type: communicationsAlarm Package: ethernetequipment.CoherentOpticalModuleTxFault Raised on class: ethernetequipment.CoherentOpticalCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CoherentModuleTxFault	Release: • 14.0
Description: The alarm is raised when a device reports Tx Fault on a coherent optical interface.		
Raising condition: (('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Network (Optical Side) Transmit') AND ('Reported Alarms'anyBit'Network (Optical Side) Transmit')))		
Remedial action: Module Tx Fault occurred.		

Table 21-50 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 21-51 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-51 ConfigurationRescueFileSaveStatus (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 21-52 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 21-53 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 21-54 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback. ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 21-55 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 21-56 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		

Table 21-56 ConfigurationRollBackStatus (rollback) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 21-57 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 21-58 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 21-59 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 21-60 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 21-61 ControlChannelDown

Alarm	Attributes	Applicable major release
Name: ControlChannelDown (8390) Type: ProtocolAlarm Package: Imp.ControlChannelDown Raised on class: Imp.ControlChannel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0

Table 21-61 ControlChannelDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a Control Channel has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A network configuration issue has been detected. Ensure the Control Channel configuration between the local node and the peer node is consistent.		

Table 21-62 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 21-63 CPMALocalInterConnectPortNotAvailable

Alarm	Attributes	Applicable major release
Name: CPMALocalInterConnectPortNotAvailable (8061) Type: communicationsAlarm Package: netw.CPMALocalInterConnectPortNotAvailable Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPMALocalInterConnectPort-NotAvailable	Release: • 12.0 • 13.0 • 14.0
Description: The CPMALocalInterConnectPortNotAvailable alarm is generated by 7950 XRS-40 when the CPM A of Master chassis cannot reach the Extended chassis through local CPM interconnect ports.		
Remedial action: Ensure that all the CPM A interconnect ports of Master and Extended chassis in the system are properly cabled together with working cables.		

Table 21-64 CPMBLocalInterConnectPortNotAvailable

Alarm	Attributes	Applicable major release
Name: CPMBLocalInterConnectPortNotAvailable (8062) Type: communicationsAlarm Package: netw.CPMBLocalInterConnectPortNotAvailable Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPMBLocalInterConnectPort-NotAvailable	Release: • 12.0 • 13.0 • 14.0
Description: The CPMBLocalInterConnectPortNotAvailable alarm is generated by 7950 XRS-40 when the CPM B of Master chassis cannot reach the Extended chassis through local CPM interconnect ports.		
Remedial action: Ensure that all the CPM B interconnect ports of Master and Extended chassis in the system are properly cabled together with working cables.		

Table 21-65 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-66 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-66 CpmProtectionExceedSapIpEntry (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-67 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-68 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtViolPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-69 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-70 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 21-71 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 21-72 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec. CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 21-73 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-74 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-75 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-76 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-77 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-78 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-79 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-80 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-81 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-82 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-83 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-84 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-85 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-86 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-87 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-88 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-89 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-90 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-91 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-92 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-93 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-94 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-95 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-96 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-97 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-98 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-99 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-100 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 21-101 DiscoveredPhysicalLinkMismatch

Alarm	Attributes	Applicable major release
Name: DiscoveredPhysicalLinkMismatch (657) Type: configurationAlarm Package: netw.DiscoveredPhysicalLinkMismatch Raised on class: netw.AbstractPhysicalLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: endPointUsedByNumerou-sLinks	Release: • 14.0

Table 21-101 DiscoveredPhysicalLinkMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one endpoint of a physical link is used as an endpoint in another physical link.		
Raising condition: ('physicalLinkMismatchConfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMismatchConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. Physical link endpoint (i.e. ports) can only be configured in one link.		

Table 21-102 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 21-103 DuplicatePhysicalLinks

Alarm	Attributes	Applicable major release
Name: DuplicatePhysicalLinks (658) Type: configurationAlarm Package: netw.DuplicatePhysicalLinks Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicatePhysicalLinkConfig-ured	Release: • 14.0
Description: The alarm is raised when there is more then one physical link configured between two endpoints.		
Raising condition: ('duplicateLinkConfigured' EQUAL 'true')		
Clearing condition: ('duplicateLinkConfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The duplicated link must be deleted.		

Table 21-104 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 21-105 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 21-106 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 21-107 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 21-108 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-109 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 21-110 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 21-111 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 21-112 EthCSF

Alarm	Attributes	Applicable major release
Name: EthCSF (3721) Type: oamAlarm Package: ethernetoam.EthCSF Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthCSF	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives a CCM frame with an interface status TLV of 'Down'.		
Remedial action: This alarm is raised when a MEP receives a CCM frame with an interface status TLV of Down.		

Table 21-113 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 21-114 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 21-115 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 21-116 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 21-117 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 21-118 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 21-119 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 21-120 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 21-121 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 21-122 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 21-123 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 21-124 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 21-125 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 21-126 FpgaFail

Alarm	Attributes	Applicable major release
Name: FpgaFail (4485) Type: equipmentAlarm Package: equipment.FpgaFail Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGAFAIL	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when FPGA download failure is detected.		
Remedial action: 1 Perform a warm reset on the card where the FPGAFAIL condition is raised.\nFor CLI config card card type shelf slot reset warm.\nFor WEBUI Select the card, click the Reboot tab, select Warm Reboot >Submit.\n2 Contact your Nokia support representative.		

Table 21-127 FpgaTimeout

Alarm	Attributes	Applicable major release
Name: FpgaTimeout (4487) Type: equipmentAlarm Package: equipment.FpgaTimeout Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FPGATIMEOUT	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when FPGA timeout is detected.		
Remedial action: 1. Perform a warm reset on the card where the FPGATIMEOUT condition is raised.		

Table 21-128 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		

Table 21-128 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 21-129 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 21-130 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 21-130 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 21-131 GmplsLspDown

Alarm	Attributes	Applicable major release
Name: GmplsLspDown (8383) Type: pathAlarm Package: gmplsuni.GmplsLspDown Raised on class: gmplsuni.GmplsLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmplsLspDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS LSP's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS LSP's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS LSP is down, despite the Administrative state being up. Check if the GMPLS path, or the LSP-path binding is down.		

Table 21-132 GmplsLspPathBindingDown

Alarm	Attributes	Applicable major release
Name: GmplsLspPathBindingDown (8384) Type: pathAlarm Package: gmplsuni.GmplsLspPathBindingDown Raised on class: gmplsuni.LspPathBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: GmplsLspPathBindingDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS LSP-path binding's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS LSP-path binding's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS LSP-path binding is down, despite the Administrative state being up. Check the failure code and fix accordingly.		

Table 21-133 GRETunnelDown

Alarm	Attributes	Applicable major release
Name: GRETunnelDown (3326) Type: serviceAlarm Package: svt.GRETunnelDown Raised on class: svt.GRETunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 14.0
Description: The alarm is raised when the IP/GRE tunnel Operational State changes to Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The situation may occur if the underlying physical port is down either because of administrative disabling or a fault on the port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable.		

Table 21-134 GroupDown

Alarm	Attributes	Applicable major release
Name: GroupDown (69) Type: ProtocolAlarm Package: rip.GroupDown Raised on class: rip.Group	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The RIP Group is down while it is administratively up. Please check RIP related configuration e.g., the RIP is not shutdown.		

Table 21-135 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-135 IgmpDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 21-136 IgmpMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxGrpSrcsLimitExceeded (4624) Type: configurationAlarm Package: igmp.IgmpMaxGrpSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxGrpSrcsLimitExceeded	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP group source for a group when the number of group sources for this group is equal to 'maxGrpSources', the maximum number of group sources per group supported on the interface.		
Remedial action: Needs to increase 'maxGrpSources' value to allow more sources on this interface.		

Table 21-137 IgmpMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxSrcsLimitExceeded (3742) Type: configurationAlarm Package: igmp.IgmpMaxSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxSrcsLimitExceeded	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt is made to configure an IGMP source for a group when the number of sources for this group is equal to 'maxSources', the maximum number of sources per group supported on the interface.		
Remedial action: Needs to increase 'maxSources' value to allow more sources on this interface.		

Table 21-138 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 21-139 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 21-140 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 21-141 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 21-142 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 21-143 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis. PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 21-144 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 21-145 InstanceDown (vrrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: vrrp.InstanceDown Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a VRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the instance configuration		

Table 21-146 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 21-147 InterChassisCommunicationDown

Alarm	Attributes	Applicable major release
Name: InterChassisCommunicationDown (8067) Type: communicationsAlarm Package: netw.InterChassisCommunicationDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InterChassisCommunication-Down	Release: • 12.0 • 13.0 • 14.0
Description: The InterChassisCommunicationDown alarm is generated by 7950 XRS-40 when the active CPM of Master chassis cannot reach the Extended (far-end) chassis. The resources on the far-end chassis are not available, this event indicates that the CPM, SFM and XCM cards in the far-end chassis will reboot and remain operationally down Until communications are re-established.		
Remedial action: Ensure that all the CPM (A & B) interconnect ports of Master and Extended chassis in the system are properly cabled together with working cables.		

Table 21-148 InterConnectPortDDMFailure

Alarm	Attributes	Applicable major release
Name: InterConnectPortDDMFailure (5621) Type: communicationsAlarm Package: equipment.InterConnectPortDDMFailure Raised on class: equipment.InterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InterConnectPortDDMFailure	Release: • 12.0 • 13.0 • 14.0
Description: The InterConnectPortDDMFailure alarm is generated by 7950 XRS-40 when a small form factor (SFF) connector in a inter connect port that supports Digital Diagnostic Monitoring (DDM) enters failed state.		

Table 21-148 InterConnectPortDDMFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: The InterConnectPortDDMFailure alarm is generated when a small form factor (SFF) connector in a inter connect port that supports Digital Diagnostic Monitoring (DDM) enters failed state, please check whether the SFF is connected properly and it functions properly, rectify any issues it may have.		

Table 21-149 InterConnectPortLinkDown

Alarm	Attributes	Applicable major release
Name: InterConnectPortLinkDown (5622) Type: communicationsAlarm Package: equipment.InterConnectPortLinkDown Raised on class: equipment.InterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InterConnectPortLinkDown	Release: • 12.0 • 13.0 • 14.0
Description: The InterConnectPortLinkDown alarm is generated by 7950 XRS-40 when the interconnect port is not operational. The reason may be a cable connected incorrectly, a disconnected cable, a faulty cable, or a misbehaving interconnect port.		
Raising condition: (('Operational State' EQUAL 'No Link') AND ('SFF Status' EQUAL 'Operational'))		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Ensure that all the interconnect ports of Master and Extended chassis in the system are properly cabled together with working cables also manual verification, testing of each interconnect port and a replacement of cabling may be required for fully functional operation.		

Table 21-150 InterConnectPortMisconnected

Alarm	Attributes	Applicable major release
Name: InterConnectPortMisconnected (5623) Type: communicationsAlarm Package: equipment.InterConnectPortMisconnected Raised on class: equipment.InterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InterConnectPortMiscon-nected	Release: • 12.0 • 13.0 • 14.0
Description: The InterConnectPortMisconnected alarm is generated by 7950 XRS-40 when interconnect ports are misconnected, master chassis interconnect ports should always be connected to appropriate extended chassis interconnect port, there is a misconnection hence this alarm has been raised.		
Raising condition: ('Operational State' EQUAL 'Invalid Connection')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Inter connect ports connections are invalid, source and target ports are misconnected, please connect appropriate source and target ports. Please refer the nodal documentation to know details about which ports in master and extended chassis should be to be connected.		

Table 21-151 InterConnectPortSFFFailure

Alarm	Attributes	Applicable major release
Name: InterConnectPortSFFFailure (5624) Type: equipmentAlarm Package: equipment.InterConnectPortSFFFailure Raised on class: equipment.InterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InterConnectPortSFFFailure	Release: • 12.0 • 13.0 • 14.0
Description: The SFFFailure alarm is generated by 7950 XRS-40 when SFF of the interconnect port has failed, this is has been indicated by the field SFFStatus having value read-error.		
Raising condition: (('SFF Status' NOT EQUAL 'Not Equipped') AND ('SFF Status' NOT EQUAL 'Operational') AND ('SFF Status' NOT EQUAL 'SFP Unsupported'))		
Clearing condition: (('SFF Status' EQUAL 'Not Equipped') OR ('SFF Status' EQUAL 'Operational'))		
Remedial action: The Small Form Factor (SFF) used in interconnect port has failed, please use the appropriate SFF which Nokia has recommended, if the SFF is correct please remove and re-insert the SFF device. If the problem persists then replace the SFF device.		

Table 21-152 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 21-153 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 21-154 InterfaceDown (vprn)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vprn.InterfaceDown Raised on class: vprn.IPMirrorInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an interface is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 21-155 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-156 IntTempLow

Alarm	Attributes	Applicable major release
Name: IntTempLow (3361) Type: equipmentAlarm Package: equipment.IntTempLow Raised on class: equipment.CardSlot	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IntTempLow	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when Card under temperature is detected.		
Remedial action: Ensure that no environmental issues are present where the network element resides.Resolve any existing issues.Verify if other cards in the shelf report temperatures near their lower limit (within 10ï¿½ C).Replace the alarmed card.		

Table 21-157 IOMEventOverflow

Alarm	Attributes	Applicable major release
Name: IOMEventOverflow (5617) Type: equipmentAlarm Package: equipment.IOMEventOverflow Raised on class: equipment.BaseCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMEventOverflow	Release: • 12.0 • 13.0 • 14.0

Table 21-157 IOMEventOverflow (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is generated when tmnxIomResStateClr, tmnxIomResExhausted and tmnxIomResHighLimitReached occur more than 200 times because of resource usage fluctuation. The IOM raises the final trap to indicate overflow and stops logging traps.		
Remedial action: Informational - The alarm will be cleared when the CPM polls the IOM for traps and the overflow is cleared by logging an overflow-clear on a particular card.		

Table 21-158 IOMResUtilizationLimit

Alarm	Attributes	Applicable major release
Name: IOMResUtilizationLimit (5618) Type: equipmentAlarm Package: equipment.IOMResUtilizationLimit Raised on class: equipment.BaseCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IOMResHighLimitReached Applicable probable causes: • IOMResHighLimitReached • IOMResExhausted	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is generated when the type of resources on IOM as specified by tmnxIomResourceType has reached the value of tmnxIomResourceLimitPct.		
Remedial action: Informational - The alarm will be cleared when the type of resources on IOM as specified by tmnxIomResourceType has dropped back down below the value of tmnxIomResourceLimitPct.		

Table 21-159 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 21-160 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 21-161 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 21-162 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 21-163 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 21-164 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 21-165 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 21-166 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 21-167 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 21-168 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 21-169 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 21-170 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 21-171 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-172 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 21-173 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 21-174 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 21-175 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 21-176 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 21-177 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 21-178 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 21-179 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 21-180 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 21-181 LSRPATHDown

Alarm	Attributes	Applicable major release
Name: LSRPATHDown (4898) Type: pathAlarm Package: mplstp.LSRPATHDown Raised on class: mplstp.TPLSRPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSRPATHDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSR Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSR Path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSR Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the forward and reverse labels are set and the Out-Link interface is operationally up.		

Table 21-182 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 21-183 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 21-184 macMoveRateExceededNonBlock (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceededNonBlock Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency even when limitMacMove(sdp-BindTlsLimitMacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 21-185 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis.MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 21-186 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 21-187 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MC endpoint is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 21-188 MemberDown

Alarm	Attributes	Applicable major release
Name: MemberDown (8385) Type: communicationsAlarm Package: gmplsuni.MemberDown Raised on class: gmplsuni. TunnelGroupEndpointMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MemberDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS tunnel group endpoint member's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS tunnel group endpoint member's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS tunnel group endpoint member is down, despite the Administrative state being up. Check with the Reason Down Flags for more details.		

Table 21-189 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 21-190 MepFacilityFault (lag)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: lag.MepFacilityFault Raised on class: lag.Interface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 21-191 MepFacilityFault (rtr)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: rtr.MepFacilityFault Raised on class: rtr.NetworkInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 21-192 MepFacilityFault (equipment)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: equipment.MepFacilityFault Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 21-193 MepFacilityFault (service)

Alarm	Attributes	Applicable major release
Name: MepFacilityFault (11101) Type: oamAlarm Package: service.MepFacilityFault Raised on class: service.AccessInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MepFacilityFault	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: [CAUSE] The tmnxDot1agCfmMepFcltyFaultRaise notification is generated when the associated facility MEP dot1agCfmMepHighestPrDefect has increased. [EFFECT] This notification can be used to correlate the ETH_CFM dot1agCfmFaultAlarm event and the related IF-MIB::linkDown notification caused by the failure of the facility MEP. [RECOVERY] Follow the recovery for the dot1agCfmFaultAlarm and the related IF-MIB::linkDown caused by the failure of the facility MEP.		
Remedial action: Follow the recovery for the CfmFaultAlarm and the related Interface linkDown caused by the failure of the facility MEP.		

Table 21-194 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 21-195 MldDown

Alarm	Attributes	Applicable major release
Name: MldDown (587) Type: ProtocolAlarm Package: mld.MldDown Raised on class: mld.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MLD site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the base router and system are configured correctly.		

Table 21-196 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 21-197 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 21-198 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 21-199 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 21-200 MsdpDown

Alarm	Attributes	Applicable major release
Name: MsdpDown (353) Type: ProtocolAlarm Package: msdp.MsdpDown Raised on class: msdp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MSDP site is administratively down. The alarm clears when the site is administratively up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the MSDP site.		

Table 21-201 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 21-202 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 21-203 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 21-204 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 21-205 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 21-206 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-207 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 21-208 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 21-209 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 21-210 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 21-211 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 21-212 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 21-213 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 21-214 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 21-215 NoSFMConfigured

Alarm	Attributes	Applicable major release
Name: NoSFMConfigured (11179) Type: equipmentAlarm Package: netw.NoSFMConfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoSFMConfigured	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when none of the SFM are configured.		
Remedial action: This alarm indicates that none of the SFM is configured. Please configured a SFM.		

Table 21-216 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-216 NTPOperDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 21-217 OesRedundancyFail

Alarm	Attributes	Applicable major release
Name: OesRedundancyFail (11111) Type: equipmentAlarm Package: equipment.OesRedundancyFail Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RedundancyFail	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when when the inactive equipment controller card in the OES is not providing redundancy protection.		
Remedial action: Check for the Redundancy demerit in the detailed information of the chassis indicated.		

Table 21-218 OFFlowEntryDeploymentCreateFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentCreateFailed (5405) Type: processingErrorAlarm Package: openflow. OFFlowEntryDeploymentCreateFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeploymentCreateFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Creation Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Creation Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects creation of the flow.		

Table 21-219 OFFlowEntryDeploymentDeleteFailed

Alarm	Attributes	Applicable major release
Name: OFFlowEntryDeploymentDeleteFailed (5406) Type: processingErrorAlarm Package: openflow.OFFlowEntryDeploymentDeleteFailed Raised on class: openflow.OFAbstractFlowEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFFlowEntryDeployment-DeleteFailed	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the flow entry deployment create has failed.		
Raising condition: (('Deployment Status' EQUAL 'Deletion Failed'))		
Clearing condition: (('Deployment Status' NOT EQUAL 'Deletion Failed'))		
Remedial action: This alarm is raised when the OpenFlow switch rejects deletion of the flow.		

Table 21-220 OFLogicalPortStatusMplsTpNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusMplsTpNotSet (5407) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusMplsTpNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusMplsTp-NotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the MPLS-TP flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'rsvp-te'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'rsvp-te'))		
Remedial action: When MPLS-TP is not set, OpenFlow port status will not be received by SAM.		

Table 21-221 OFLogicalPortStatusRsvpTeNotSet

Alarm	Attributes	Applicable major release
Name: OFLogicalPortStatusRsvpTeNotSet (5408) Type: equipmentAlarm Package: openflow.OFLogicalPortStatusRsvpTeNotSet Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFLogicalPortStatusRs-vpTeNotSet	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the RSVP-TE flag is not set in the Logical Port Status.		
Raising condition: (('Logical Port Status' EQUAL '0L') OR ('Logical Port Status' EQUAL 'mpls-tp'))		
Clearing condition: (('Logical Port Status' NOT EQUAL '0L') AND ('Logical Port Status' NOT EQUAL 'mpls-tp'))		
Remedial action: When RSVP-TE is not set, OpenFlow port status will not be received by SAM.		

Table 21-222 OFSwitchDown

Alarm	Attributes	Applicable major release
Name: OFSwitchDown (5409) Type: equipmentAlarm Package: openflow.OFSwitchDown Raised on class: openflow.OFSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OFSwitchDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Operational State of an OFSwitch is Down and the Administrative State is Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm is raised when the OpenFlow switch has gone down.		

Table 21-223 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-224 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 21-225 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 21-226 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 21-227 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 21-228 PccRuleInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: PccRuleInsertedFltrEntryDropped (11059) Type: configurationAlarm Package: aclfilter.PccRuleInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a request to insert a filter entry is not successful for a PCC rule application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for PCC rule application. Check the configuration filter entry.		

Table 21-229 PccRuleInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: PccRuleInsertSpaceThresholdAlarm (11058) Type: configurationAlarm Package: aclfilter.PccRuleInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a PCC rule application insert range.		
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for PCC rule application. Make an adjusted to the watermarks or to the filter.		

Table 21-230 PeerConnectionDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: msdp.PeerConnectionDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-230 PeerConnectionDown (msdp) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the connectionState of this peer changes from Established to a state other than Established. The alarm clears when the connectionState of this peer returns to the Established state.		
Raising condition: (('connectionState' NOT EQUAL 'Established') AND ('administrativeState' EQUAL 'Up'))		
Clearing condition: (('connectionState' EQUAL 'Established') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Check the configurations of the peer routers.		

Table 21-231 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 21-232 PeerDown (gmplsuni)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: gmplsuni.PeerDown Raised on class: gmplsuni.Peer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS peer's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS peer's Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS peer is down, despite the Administrative state being up. Check if the associated LMP peer or the GMPLS tunnel group endpoint is down.		

Table 21-233 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-234 PeerDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: msdp.PeerDown Raised on class: msdp.CommonPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Administrative State of a peer changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('administrativeState' EQUAL 'Down'))		
Clearing condition: (('administrativeState' NOT EQUAL 'Down'))		
Remedial action: Turn up the Peer.		

Table 21-235 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-236 PeerGroupDown (msdp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: msdp.PeerGroupDown Raised on class: msdp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Administrative State of a peer group changes from Up to Down. The alarm clears when the Administrative State returns to Up.		
Raising condition: (('Administrative State' EQUAL 'Down'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Down'))		
Remedial action: Turn up the Group.		

Table 21-237 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 21-238 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 21-239 PhysicalLinkPortsMisconfigured

Alarm	Attributes	Applicable major release
Name: PhysicalLinkPortsMisconfigured (239) Type: configurationAlarm Package: netw.PhysicalLinkPortsMisconfigured Raised on class: netw.AbstractPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: physicalLinkPortsMisconfig-ured	Release: • 14.0
Description: The alarm is raised when there is an MTU size mismatch between a link endpoint and a port. The alarm clears when the MTUs match.		
Raising condition: ('physicalLinkMisconfigured' EQUAL 'true')		
Clearing condition: ('physicalLinkMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The MTU value(s) on the link endpoint and port must be changed such that they match.		

Table 21-240 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 21-241 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 21-242 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 21-243 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 21-244 PowerCapacityExceeded

Alarm	Attributes	Applicable major release
Name: PowerCapacityExceeded (5146) Type: equipmentAlarm Package: equipment.PowerCapacityExceeded Raised on class: equipment.PowerManagementZone	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerCapacityExceeded	Release: • 11.0.R4
Description: The PowerCapacityExceeded alarm is generated when a device needs power to boot, but there is not enough power capacity to support the device.		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 21-245 PowerLostCapacity

Alarm	Attributes	Applicable major release
Name: PowerLostCapacity (5147) Type: equipmentAlarm Package: equipment.PowerLostCapacity Raised on class: equipment.PowerManagementZone	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerLostCapacity	Release: • 11.0.R4
Description: The PowerLostCapacity alarm is generated when a power supply fails or is removed which puts the system in an overloaded situation.		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 21-246 PowerOverloadState

Alarm	Attributes	Applicable major release
Name: PowerOverloadState (5148) Type: equipmentAlarm Package: equipment.PowerOverloadState Raised on class: equipment.PowerManagementZone	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerOverloadState	Release: • 11.0.R4
Description: The PowerOverloadState alarm is generated when the overloaded power capacity can not support the power requirements and there are no further devices that can be powered off.		
Remedial action: To recover from this state, the customer is requested to add power capacity, or to manually shutdown devices until the power capacity meets the power needs.		

Table 21-247 PowerSafetyAlertThreshold

Alarm	Attributes	Applicable major release
Name: PowerSafetyAlertThreshold (5149) Type: thresholdCrossed Package: equipment.PowerSafetyAlertThreshold Raised on class: equipment.PowerManagementZone	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSafetyAlertThreshold-Crossed	Release: • 11.0.R4
Description: The PowerSafetyAlertThreshold notification is generated when the system power capacity drops below the configured safety alert threshold.		
Remedial action: Decrease the safety alert threshold or reduce the power utilization below safety alert threshold.		

Table 21-248 PowerSafetyLevelThreshold

Alarm	Attributes	Applicable major release
Name: PowerSafetyLevelThreshold (5150) Type: thresholdCrossed Package: equipment.PowerSafetyLevelThreshold Raised on class: equipment.PowerManagementZone	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSafetyLevelThreshold-Crossed	Release: • 11.0.R4
Description: The PowerSafetyLevelThreshold notification is generated when the peak nodal power consumption exceeds the configured safety level threshold.		
Remedial action: Increase the safety level threshold or reduce the power utilization below safety level threshold.		

Table 21-249 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-250 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-251 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-252 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-253 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 21-254 PowerSupplyInputFeedDownAlarm

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDownAlarm (5154) Type: equipmentAlarm Package: equipment. PowerSupplyInputFeedDownAlarm Raised on class: equipment.PowerSupply	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('Input Feed Status' EQUAL 'Input A Down') OR ('Input Feed Status' EQUAL 'Input B Down') OR (('Input Feed Status'allBits'Input A Down') AND ('Input Feed Status'allBits'Input B Down')))		
Clearing condition: ('Input Feed Status' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power		

Table 21-255 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-256 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-257 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 21-258 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 21-259 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 21-260 ProvPowerCapacity

Alarm	Attributes	Applicable major release
Name: ProvPowerCapacity (5182) Type: equipmentAlarm Package: equipment.ProvPowerCapacity Raised on class: equipment.PowerManagementZone	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: provPowerCapacity	Release: • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The ProvisionedPowerCapacity alarm is generated if a power zone's provisioned power capacity can no longer support configured devices.		
Remedial action: The system can no longer support configured devices. Power capacity is not sufficient enough to operate all the configured devices. Add more PEQs or delete some devices		

Table 21-261 PXCAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: PXCAdministrativelyDown (11185) Type: equipmentAlarm Package: pxc.PXCAdministrativelyDown Raised on class: pxc.PortCrossConnect	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portCrossConnectAdministra-tivelyDown	Release: • 14.0
Description: The alarm is raised when the PXC AdministrativelyDown.		
Raising condition: ('Administrative State' EQUAL 'Down')		

Table 21-261 PXCAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Administrative State' EQUAL 'Up'))		
Remedial action: Informational - PortCrossConnect AdministrativelyDown.		

Table 21-262 PXCDown

Alarm	Attributes	Applicable major release
Name: PXCDown (11186) Type: equipmentAlarm Package: pxc.PXCDown Raised on class: pxc.PortCrossConnect	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperablePortCrossConnect	Release: • 14.0
Description: The alarm is raised when the PXC is OperationallyDown.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: This alarm indicates an inoperable PortCrossConnect. Either the associated PhysicalPort or PortCrossConnectSub-ports are down.		

Table 21-263 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 21-264 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 21-265 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 21-266 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 21-267 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 21-268 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 21-269 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 21-270 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-271 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfigured	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 21-272 RPKISessionNotEstablished

Alarm	Attributes	Applicable major release
Name: RPKISessionNotEstablished (8136) Type: communicationsAlarm Package: rtr.RPKISessionNotEstablished Raised on class: rtr.RpkiSession	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RPKISessionNotEstablished	Release: • 12.0 • 13.0 • 14.0
Description: The notification alarm is raised when the RPKI Session is not established.		
Raising condition: (('Session State' NOT EQUAL 'Established'))		
Clearing condition: (('Session State' EQUAL 'Established'))		
Remedial action: Make sure that the Cache server is reachable and is configured properly.		

Table 21-273 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 21-274 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0

Table 21-274 RxSectionSynchronizationError (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 21-275 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 21-276 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		

Table 21-276 S2LPathDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 21-277 SapDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosDynamicExceeded (4890) Type: securityServiceOrMechanismViolation Package: service.SapDDosDynamicExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the protocol on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpDynamicExcd trap) and the alarm status is set as non-conformant When the SAP starts hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP completes hold-down period for an exceeding protocol (on receiving sapDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 21-278 SapDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosLocMonitorExceeded (4891) Type: securityServiceOrMechanismViolation Package: service.SapDDosLocMonitorExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the SAP (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular SAP has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 21-279 SapDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: SapDDosStaticExceeded (4892) Type: securityServiceOrMechanismViolation Package: service.SapDDosStaticExceeded Raised on class: service.AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the static-policer on a particular SAP has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving sapDcpStaticExcd trap) and the alarm status is set as non-conformant. When the SAP starts hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the SAP ends hold-down period for the exceeding static-policer (on receiving sapDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the SAP has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving sapDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected SAP may be required.		

Table 21-280 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 21-281 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 21-282 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 21-283 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 21-284 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 21-285 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 21-286 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-287 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 21-288 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 21-289 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-290 ServerMaxLeasesReached

Alarm	Attributes	Applicable major release
Name: ServerMaxLeasesReached (3316) Type: configurationAlarm Package: netw.ServerMaxLeasesReached Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrMaxLeasesReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the maximum number of leases allocated by local DHCP server is reached.		
Remedial action: Informational - this alarm indicates that the maximum number of leases allocated by a local DHCP server was reached. The address ranges for existing address pools should be extended or a new address pool should be configured for the local DHCP server.		

Table 21-291 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 21-292 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 21-293 SFMInterconnectPortDegraded

Alarm	Attributes	Applicable major release
Name: SFMInterconnectPortDegraded (5647) Type: communicationsAlarm Package: equipment.SFMInterconnectPortDegraded Raised on class: equipment.SFMInterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SFMInterconnectPortDegraded	Release: • 12.0 • 13.0 • 14.0
Description: The SFMInterconnectPortDegraded alarm is generated by 7950 XRS-40 when the system has detected a reduction in switch fabric capacity because of degrade in a particular SFM interconnect port associated to the switch fabric. This is indicated through the field SfmIcPortDegradeState, the value of the field would not be None in this condition. The value degraded indicates switch fabric capacity on this port is reduced, but SFM interconnect port can still carry some traffic but not all the full capacity of the interconnect port.		
Raising condition: ('Fabric Degrade State' NOT EQUAL 'None')		
Clearing condition: ('Fabric Degrade State' EQUAL 'None')		
Remedial action: Switch fabric capacity is reduced due to the degradation in associated SFM interconnect port, this may not cause any impact to service because of redundancy in the fabric. Although it may not be possible to maintain full service, the SFM interconnection port and attached cable may be the cause for the degradation, replacing the affected components may restore some fabric capacity.		

Table 21-294 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-295 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 21-296 SonetPathAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: SonetPathAlarmIndicationSignal (129) Type: communicationsAlarm Package: sonetequipment. SonetPathAlarmIndicationSignal Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathAlarmIndicationSignal	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Indication Signal') AND ('Report Alarms'anyBit'Path Alarm Indication Signal')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-297 SonetPathB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathB3Error (132) Type: communicationsAlarm Package: sonetequipment.SonetPathB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathB3Error	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition because of b3 errors. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path B3 error') AND ('Report Alarms'anyBit'Path B3 error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-298 SonetPathLossOfCodegroupDelineationError

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfCodegroupDelineationError (248) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfCodegroupDelineationError Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfCodegroupDelineationError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLCD error. The alarm corresponds to the plcd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Codegroup Delineation Error') AND ('Report Alarms'anyBit'Path Loss of Codegroup Delineation Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-299 SonetPathLossOfPointer

Alarm	Attributes	Applicable major release
Name: SonetPathLossOfPointer (130) Type: communicationsAlarm Package: sonetequipment.SonetPathLossOfPointer Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathLossOfPointer	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PLOP error. The alarm corresponds to the plop alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Loss of Pointer') AND ('Report Alarms'anyBit'Path Loss of Pointer')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-300 SonetPathPayloadMismatch

Alarm	Attributes	Applicable major release
Name: SonetPathPayloadMismatch (133) Type: communicationsAlarm Package: sonetequipment.SonetPathPayloadMismatch Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathPayloadMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a PPLM error on a channel, after which the channel is set operationally down. The alarm corresponds to the pplm alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Payload Mismatch') AND ('Report Alarms'anyBit'Path Payload Mismatch')))		
Remedial action: Informational only.		

Table 21-301 SonetPathRemoteB3Error

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteB3Error (134) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteB3Error Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteB3Error	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path error condition that a remote NE raises because of b3 errors received from the local NE. The alarm corresponds to the prei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote B3 Error') AND ('Report Alarms'anyBit'Path Remote B3 Error')))		
Remedial action: Check the remote NE is configured correctly and its physical layer cabling is operating correctly.		

Table 21-302 SonetPathRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: SonetPathRemoteDefectIndication (131) Type: communicationsAlarm Package: sonetequipment.SonetPathRemoteDefectIndication Raised on class: sonetequipment.SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathRemoteDefectIndication	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a remote PAIS error. The alarm corresponds to the pais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Remote Defect Indication') AND ('Report Alarms'anyBit'Path Remote Defect Indication')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-303 SonetPathUnequippedPathError

Alarm	Attributes	Applicable major release
Name: SonetPathUnequippedPathError (143) Type: communicationsAlarm Package: sonetequipment. SonetPathUnequippedPathError Raised on class: sonetequipment. SonetChannelMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pathUnequippedPathError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports a path unequipped error. The alarm corresponds to the Path Alarm Unequipped Path Error alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Path Alarm Unequipped Path Error') AND ('Report Alarms'anyBit'Path Alarm Unequipped Path Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-304 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 21-305 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 21-306 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 21-307 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 21-308 StpExceptionCondition

Alarm	Attributes	Applicable major release
Name: StpExceptionCondition (297) Type: AccessInterfaceAlarm Package: l2fwd.StpExceptionCondition Raised on class: l2fwd.AccessInterfaceStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP exception condition, for example, one-way communication or a downstream loop. The alarm clears when the STP condition changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 21-309 StpRootGuardViolation

Alarm	Attributes	Applicable major release
Name: StpRootGuardViolation (503) Type: AccessInterfaceAlarm Package: l2fwd.StpRootGuardViolation Raised on class: l2fwd.AccessInterfaceStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: spanningTreeTopology-Changed	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SAP detects an STP root guard violation.		
Raising condition: ('Root Guard Violation' EQUAL 'true')		
Clearing condition: ('Root Guard Violation' NOT EQUAL 'true')		
Remedial action: Set 'Root Guard' to false if not necessary.		

Table 21-310 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 21-311 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 21-312 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 21-313 TeLinkDown (gmplsuni)

Alarm	Attributes	Applicable major release
Name: TeLinkDown (8386) Type: ProtocolAlarm Package: gmplsuni.TeLinkDown Raised on class: gmplsuni.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when the GMPLS TE link's Administrative State is Up and the Operational State is Down. The alarm clears when the GMPLS TE link's Operational State changes to Up or the Administrative State changes to Down.		

Table 21-313 TeLinkDown (gmplsuni) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the GMPLS TE link is down, despite the Administrative state being up. Check if the associated LMP TE link or the GMPLS tunnel group endpoint is down.		

Table 21-314 TeLinkDown (lmp)

Alarm	Attributes	Applicable major release
Name: TeLinkDown (8386) Type: ProtocolAlarm Package: lmp.TeLinkDown Raised on class: lmp.TeLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 13.0 • 14.0
Description: The alarm is raised when a Traffic-Engineering Link has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A network configuration issue has been detected. Ensure the Traffic-Engineering Link configuration between the local node and the peer node is consistent.		

Table 21-315 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 21-316 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 21-317 TPLSPDown

Alarm	Attributes	Applicable major release
Name: TPLSPDown (4900) Type: pathAlarm Package: mplstp.TPLSPDown Raised on class: mplstp.TPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP is down, despite the Administrative state being up. Review the configuration and make sure that the destination information is set correctly and that the Administrative state is up.		

Table 21-318 TPLSPPATHDown

Alarm	Attributes	Applicable major release
Name: TPLSPPATHDown (4901) Type: pathAlarm Package: mplstp.TPLSPPATHDown Raised on class: mplstp.TPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TPLSPPATHDown	Release: • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the TP LSP Path Administrative State is Up and the Operational State is Down. The alarm clears when the TP LSP Path Operational State changes to Up or the Administrative State changes to Down.		

Table 21-318 TPLSPPATHDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The Operational state of the TP LSP Path is down, despite the Administrative state being up. Review the configuration and make sure that the Administrative state is up, the egress and ingress labels are set and the Out-Link interface is operationally up.		

Table 21-319 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 21-320 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		

Table 21-320 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 21-321 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 21-322 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 21-323 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 21-324 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 21-325 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 21-326 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 21-327 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 21-328 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 21-329 UnsupportedSFFinInterConnectPort

Alarm	Attributes	Applicable major release
Name: UnsupportedSFFinInterConnectPort (5659) Type: equipmentAlarm Package: equipment. UnsupportedSFFinInterConnectPort Raised on class: equipment.InterConnectPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnsupportedSFFinInterConnectPort	Release: • 12.0 • 13.0 • 14.0
Description: The UnsupportedSFFinIntetrConnectPort alarm is generated by 7950 XRS-40 when SFF is not recognized by the system or wrong SFF model different from which Nokia has recommended is used. The SFF device is not operational and the associated interconnect port cannot be used.		
Raising condition: ('Operational State' EQUAL 'Unsupported SFF')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: The Small Form Factor (SFF) used in interconnect port seems to be unsupported type, please use the appropriate SFF which Nokia has recommended, if the SFF is correct please remove and re-insert the SFF device. If the problem persists then replace the SFF device.		

Table 21-330 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 21-331 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 21-332 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 21-333 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 21-334 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 21-335 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-336 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 21-337 VRtrIfDDosDynamicExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosDynamicExceeded (4887) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosDynamicExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the protocol on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpDynamicExcd trap) and the alarm status is set as non-conformant When the network interface starts hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface completes hold-down period for an exceeding protocol (on receiving vRtrIfDcpDynamicHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the protocol for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpDynamicConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 21-338 VRtrIfDDosLocMonitorExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosLocMonitorExceeded (4888) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosLocMonitorExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system will attempt to allocate dynamic enforcement policers (on receiving sapDcpLocMonExcd trap), and the alarm status is set as non-conformant When all dynamic enforcement policers associated with a non-conformant local-monitoring-policer have been successfully allocated for the network interface (on receiving sapDcpLocMonExcdAllDynAlloc trap), the alarm status will be changed into non-conformant(Located All). When the local-monitoring-policer for a particular network interface has transitioned from a conformant state to a non-conformant state and the system cannot allocate all the dynamic enforcement policers associated with the distributed CPU protection policy (on receiving sapDcpLocMonExcdDynResource trap), the alarm status will be changed into non-conformant(Cannot Allocate All). When all the previously allocated dynamic enforcement policers for a particular local-monitoring-policer on the associated distributed CPU protection policy have been freed up and all the protocols are once again being monitored by local-monitor (on receiving sapDcpLocMonExcdAllDynFreed trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 21-339 VRtrIfDDosStaticExceeded

Alarm	Attributes	Applicable major release
Name: VRtrIfDDosStaticExceeded (4889) Type: securityServiceOrMechanismViolation Package: rtr.VRtrIfDDosStaticExceeded Raised on class: rtr.VirtualInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExceedingPolicingParameters	Release: • 11.0 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the static-policer on a particular network interface has been detected as non-conformant to the associated distributed CPU protection policy parameters (on receiving vRtrIfDcpStaticExcd trap) and the alarm status is set as non-conformant. When the network interface starts hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHold-DownStart trap), the alarm status will change into non-conformant(Hold Down Start). When the network interface ends hold-down period for the exceeding static-policer (on receiving vRtrIfDcpStaticHoldDownEnd trap), the alarm status will be changed into non-conformant(Hold Down End). When the static-policer for the network interface has been detected as conformant for a period of the configured detection-time after having been previously detected as exceeding and completed any hold-down period (on receiving vRtrIfDcpStaticConform trap), the alarm will be cleared.		
Remedial action: Appropriate configuration changes to the distributed CPU protection policy or to the affected network interface may be required.		

Table 21-340 WaveTrackerEncoderDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderDegrade (821) Type: communicationsAlarm Package: ethernetequipment.WaveTrackerEncoderDegrade Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderDegrade	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Degrade') AND ('Reported Alarms'anyBit'Encoder Degrade')))		
Remedial action: The OT or SVAC card has detected a DSP failure and this means that the wavelength tracker encode power control is compromised. If this occurs during steady state operation, there is a high probability that the services carried by this OT or SVAC are unaffected. To clear this alarm, replace the card. The card replacement procedure is service affecting and should be conducted during a maintenance window.		

Table 21-341 WaveTrackerEncoderFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerEncoderFailure (822) Type: communicationsAlarm Package: ethernetequipment.WaveTrackerEncoderFailure Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EncoderFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports an encoder failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Encoder Failure') AND ('Reported Alarms'anyBit'Encoder Failure')))		
Remedial action: A cold reset, reseat, or replacement of a card is service impacting if the card is currently carrying services. If there are services currently carried over the card, it may be best to wait for a maintenance window before resetting, replacing, or reseating the card.Confirm that replacement OT or SVAC card supports the same band as the alarmed OT or SVAC card and connect all fibers to the replacement OT or SVAC card.		

Table 21-342 WaveTrackerMissingPluggableVOA

Alarm	Attributes	Applicable major release
Name: WaveTrackerMissingPluggableVOA (4618) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerMissingPluggableVOA Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingPluggableVOA	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Missing Pluggable VOA') AND ('Reported Alarms'anyBit'Missing Pluggable VOA')))		
Remedial action: Informational - no corrective action required.		

Table 21-343 WaveTrackerPowerControlDegrade

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlDegrade (823) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlDegrade Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlDegrade	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control degradation on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Degrade') AND ('Reported Alarms'anyBit'Power Control Degrade')))		
Remedial action: check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.		

Table 21-344 WaveTrackerPowerControlFailure

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlFailure (824) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlFailure	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control failure on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Failure') AND ('Reported Alarms'anyBit'Power Control Failure')))		
Remedial action: Either alarmed card has detected equipment problem or there is misfibering problem such that a light-emitting fiber has been plugged into the Tx port of aWavelength Tracker encoder-equipped transponder card.If the card is a transponder card that is equipped with aWavelength Tracker encoder, check to see that the fibering for that card is correct. Remove the fiber from the Tx port on the transponder card. If the condition clears after 20 seconds, then this is a misfibering problem.the card is an SVAC, or if there is no fibering problem on the transponder card.Disconnect all fibers on the alarmed card and Replace the card. connect all fibers to the replacement card		

Table 21-345 WaveTrackerPowerControlHighlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControlHighlimit (825) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControlHighlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControlHighlimit	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control high limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control High limit reached') AND ('Reported Alarms'anyBit'Power Control High limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 21-346 WaveTrackerPowerControllowlimit

Alarm	Attributes	Applicable major release
Name: WaveTrackerPowerControllowlimit (826) Type: communicationsAlarm Package: ethernetequipment. WaveTrackerPowerControllowlimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerControllowlimit	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when a device reports a power control low limit on a wavelength tracker interface.		
Raising condition: (('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached'))		
Clearing condition: NOT ((('Configured Alarms'anyBit'Power Control Low limit reached') AND ('Reported Alarms'anyBit'Power Control Low limit reached')))		
Remedial action: Informational - no corrective action required.		

Table 21-347 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 21-348 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 10.0 • 11.0 • 11.0.R4 • 12.0 • 13.0 • 14.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

22 8000 MDR

22.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 22-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 2.2.1
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 22-2 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 2.2.1
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 22-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.2.1
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 22-4 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.2.1
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 22-5 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 2.2.1
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		

Table 22-5 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 22-6 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 22-7 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 22-8 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 2.2.1
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 22-9 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.2.1
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 22-10 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 2.2.1

Table 22-10 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 22-11 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 22-12 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 22-13 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 22-14 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 2.2.1
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 22-15 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 2.2.1
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		

Table 22-15 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 22-16 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 22-17 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 2.2.1
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 22-18 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 2.2.1

Table 22-18 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 22-19 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 2.2.1
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 22-20 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 22-21 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 2.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 22-22 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 2.2.1
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 22-23 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 2.2.1
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 22-24 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.2.1
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 22-25 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.2.1
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 22-26 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 2.2.1
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		

Table 22-26 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 22-27 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 2.2.1
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 22-28 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 2.2.1
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 22-29 LocalAccessRequested

Alarm	Attributes	Applicable major release
Name: LocalAccessRequested (9631) Type: equipmentAlarm Package: mpr.LocalAccessRequested Raised on class: mpr.MprNeProperties	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lacRequested	Release: • 2.2.1
Description: The alarm is raised when the Local access is requested by CT		
Raising condition: (('Lac state' EQUAL 'Access Requested'))		
Clearing condition: ('Lac state' NOT EQUAL 'Access Requested')		
Remedial action: Alarm is raised when CT requests access to NE. Navigate to System settings and grant local access if needed or ignore the request and wait for the timeout to expire for alarm to clear.		

Table 22-30 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 2.2.1
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 22-31 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 22-32 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 2.2.1
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 22-33 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 2.2.1
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 22-34 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 2.2.1
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 22-35 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 2.2.1
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 22-36 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 22-37 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.2.1
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 22-38 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 2.2.1
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 22-39 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 2.2.1
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		

Table 22-39 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 22-40 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 2.2.1
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 22-41 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 22-42 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 2.2.1
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 22-43 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 2.2.1
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 22-44 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 2.2.1
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 22-44 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 22-45 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 2.2.1
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 22-46 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 2.2.1
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 22-47 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 2.2.1

Table 22-47 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 22-48 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 22-49 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.2.1
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 22-50 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.2.1
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 22-51 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 2.2.1
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 22-52 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 2.2.1
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		

Table 22-52 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 22-53 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 2.2.1
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 22-54 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 2.2.1
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 22-55 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 2.2.1
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 22-56 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 2.2.1
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 22-57 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 2.2.1
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 22-58 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 2.2.1
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 22-59 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 2.2.1
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 22-60 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 2.2.1
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 22-61 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 2.2.1
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

23 936x/996x SC access point

23.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 23-1 actionsaborted

Alarm	Attributes	Applicable major release
Name: actionsaborted (6248) Type: equipmentAlarm Package: femto.actionsaborted Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of action aborted		
Remedial action: Not available		

Table 23-2 actionsfailed

Alarm	Attributes	Applicable major release
Name: actionsfailed (6249) Type: equipmentAlarm Package: femto.actionsfailed Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of action failed		
Remedial action: Not available		

Table 23-3 actionsqueued

Alarm	Attributes	Applicable major release
Name: actionsqueued (6250) Type: equipmentAlarm Package: femto.actionsqueued Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of action queued		

Table 23-3 actionsqueued (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-4 actionsqueuedfunctionsaddobject

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsaddobject (6251) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsaddobject Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of addobject function queued		
Remedial action: Not available		

Table 23-5 actionsqueuedfunctionsbackup

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsbackup (6252) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsbackup Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of backup function queued		
Remedial action: Not available		

Table 23-6 actionsqueuedfunctionsconfigurationdownload

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsconfigurationdownload (6253) Type: equipmentAlarm Package: femto. actionsqueuedfunctionsconfigurationdownload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of configurationdownload function queued		
Remedial action: Not available		

Table 23-7 actionsqueuedfunctionsconfigurationupload

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsconfigurationupload (6254) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsconfigurationupload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of configurationupload function queued		
Remedial action: Not available		

Table 23-8 actionsqueuedfunctionsconnect

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsconnect (6255) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsconnect Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of connect function queued		
Remedial action: Not available		

Table 23-9 actionsqueuedfunctionsdeleteobject

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsdeleteobject (6256) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsdeleteobject Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of deleteobject function queued		
Remedial action: Not available		

Table 23-10 actionsqueuedfunctionsfactoryreset

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsfactoryreset (6257) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsfactoryreset Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of factoryreset function queued		

Table 23-10 actionsqueuedfunctionsfactoryreset (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-11 actionsqueuedfunctionsfirmwareupdate

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsfirmwareupdate (6258) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsfirmwareupdate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of firmwareupdate function queued		
Remedial action: Not available		

Table 23-12 actionsqueuedfunctionsgetoptions

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetoptions (6259) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetoptions Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getoptions function queued		
Remedial action: Not available		

Table 23-13 actionsqueuedfunctionsgetparameterattributes

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetparameterattributes (6260) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetparameterattributes Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getparameterattributes function queued		
Remedial action: Not available		

Table 23-14 actionsqueuedfunctionsgetparameternames

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetparameternames (6261) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetparameternames Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getparametervalues function queued		
Remedial action: Not available		

Table 23-15 actionsqueuedfunctionsgetparametervalues

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetparametervalues (6262) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getqueuedtransfers function queued		
Remedial action: Not available		

Table 23-16 actionsqueuedfunctionsgetqueuedtransfers

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetqueuedtransfers (6263) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetqueuedtransfers Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getrpcmethods function queued		
Remedial action: Not available		

Table 23-17 actionsqueuedfunctionsgetrpcmethods

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsgetrpcmethods (6264) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsgetrpcmethods Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of reboot function queued		
Remedial action: Not available		

Table 23-18 actionsqueuedfunctionsreboot

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsreboot (6265) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsreboot Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of restore function queued		
Remedial action: Not available		

Table 23-19 actionsqueuedfunctionsrestore

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsrestore (6266) Type: equipmentAlarm Package: femto.actionsqueuedfunctionsrestore Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of restore function queued		
Remedial action: Not available		

Table 23-20 actionsqueuedfunctionsscheduleinform

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionsscheduleinform (6267) Type: equipmentAlarm Package: femto. actionsqueuedfunctionsscheduleinform Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of .scheduleinform function queued		
Remedial action: Not available		

Table 23-21 actionsqueuedfunctionssetparameterattributes

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionssetparameterattributes (6268) Type: equipmentAlarm Package: femto.actionsqueuedfunctionssetparameterattributes Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of setparameterattributes function queued		
Remedial action: Not available		

Table 23-22 actionsqueuedfunctionssetparametervalues

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionssetparametervalues (6269) Type: equipmentAlarm Package: femto.actionsqueuedfunctionssetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of setparametervalues function queued		
Remedial action: Not available		

Table 23-23 actionsqueuedfunctionssetvouchers

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionssetvouchers (6270) Type: equipmentAlarm Package: femto.actionsqueuedfunctionssetvouchers Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of setvouchers function queued		
Remedial action: Not available		

Table 23-24 actionsqueuedfunctionssnmpgetparametervalues

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionssn-mpgetparametervalues (6271) Type: equipmentAlarm Package: femto.actionsqueuedfunctionssnmpgetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of snmpgetparametervalues function queued		
Remedial action: Not available		

Table 23-25 actionsqueuedfunctionssnmpsetparametervalues

Alarm	Attributes	Applicable major release
Name: actionsqueuedfunctionssn-mpsetparametervalues (6272) Type: equipmentAlarm Package: femto.actionsqueuedfunctionssnmpsetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of snmpsetparametervalues function queued		
Remedial action: Not available		

Table 23-26 actionssucceeded

Alarm	Attributes	Applicable major release
Name: actionssucceeded (6273) Type: equipmentAlarm Package: femto.actionssucceeded Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of action succeeded		
Remedial action: Not available		

Table 23-27 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 14.2

Table 23-27 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 23-28 AGPS_agpsServiceFailure

Alarm	Attributes	Applicable major release
Name: AGPS_agpsServiceFailure (5676) Type: processingErrorAlarm Package: femto.AGPS_agpsServiceFailure Raised on class: femto.AGPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Fault is raised if a failure is detected on the Assisted GPS Service		
Remedial action: The alarm will clear automatically when the problem with the interface to the AGPS server is resolved. If the problem persists, contact Nokia customer suppor		

Table 23-29 AGPS_noAGPSInfoinUEBasedAGPS

Alarm	Attributes	Applicable major release
Name: AGPS_noAGPSInfoinUEBasedAGPS (5677) Type: integrityViolation Package: femto.AGPS_noAGPSInfoinUEBasedAGPS Raised on class: femto.AGPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: informationMissing	Release: • 14.2
Description: This fault is raised when the CN request a UE based AGPS positioning, and the Small Cell fails to get the AGPS from its AGPS caching proxy.If this happen, Small cell will not be able to forward any AGPS information to UE, and thus will not be able to perform AGPS based localization.		
Remedial action: Check the connection between AP and AGPS caching proxy		

Table 23-30 AGPS_notEnoughAGPSInfo

Alarm	Attributes	Applicable major release
Name: AGPS_notEnoughAGPSInfo (5678) Type: integrityViolation Package: femto.AGPS_notEnoughAGPSInfo Raised on class: femto.AGPS	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: informationMissing	Release: • 14.2

Table 23-30 AGPS_notEnoughAGPSInfo (continued)

Alarm	Attributes	Applicable major release
Description: This fault indicates that the number of GPS satellites for which navigations models are available to the iSMLC is insufficient. This impacts the iSMLC's capability to provide assistance data, if the error persists over a longer period of time.If insufficient amount of GPS navigation data is available, AGPS positioning MIGHT fail and consequently the positioning accuracy are compromised.The iSMLC continuously receives navigation models for less than 4 GPS satellites over a period of 10 minutes.		
Remedial action: Configure more assitance data in AGPS cache proxy.		

Table 23-31 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 14.2
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 23-32 alarmOverload

Alarm	Attributes	Applicable major release
Name: alarmOverload (11165) Type: equipmentAlarm Package: femto.alarmOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for alarms.		
Raising condition: (('Alarm OverLoad' EQUAL 'true'))		
Clearing condition: (('Alarm OverLoad' EQUAL 'false'))		
Remedial action: Threshold exceeds for alarms		

Table 23-33 applicationalarmOverload

Alarm	Attributes	Applicable major release
Name: applicationalarmOverload (11166) Type: equipmentAlarm Package: femto.applicationalarmOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for application alarms.		
Remedial action: Threshold exceeds for application alarms		

Table 23-34 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 14.2
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 23-35 AVCNOverload

Alarm	Attributes	Applicable major release
Name: AVCNOverload (11139) Type: equipmentAlarm Package: femto.AVCNOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for AVCN.		
Raising condition: (('AVCN OverLoad' EQUAL 'true'))		
Clearing condition: (('AVCN OverLoad' EQUAL 'false'))		
Remedial action: Threshold exceeds for AVCN		

Table 23-36 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 14.2
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 23-37 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 14.2
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 23-38 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 14.2
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 23-38 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 23-39 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 14.2
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 23-40 BSRlinkloss

Alarm	Attributes	Applicable major release
Name: BSRlinkloss (8173) Type: communicationsAlarm Package: femto.BSRlinkloss Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: BSR is not reachable from HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes.		

Table 23-41 BSRSubscriberTraceConfig_subscriberTraceRecordingSessionFailure

Alarm	Attributes	Applicable major release
Name: BSRSubscriberTraceConfig_ subscriberTraceRecordingSessionFailure (5801) Type: processingErrorAlarm Package: femto.BSRSubscriberTraceConfig_ subscriberTraceRecordingSessionFailure Raised on class: femto.FemtoSubscriberTraceConfig	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Failure to start a trace recording session due to any problem.		
Remedial action: Configure the IMSI attribute of class SubscriberTrace and perform the call trace recording session.Verify the call of the IMSI that to be traced.The alarms gets cleared manually from the OAM system once the call is traced.		

Table 23-42 BSRSubscriberTraceConfig_subscriberTraceUploadFailure

Alarm	Attributes	Applicable major release
Name: BSRSubscriberTraceConfig_ subscriberTraceUploadFailure (5802) Type: communicationsAlarm Package: femto.BSRSubscriberTraceConfig_ subscriberTraceUploadFailure Raised on class: femto.FemtoSubscriberTraceConfig	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: Failure to transferring SubscriberTrace files even after retries.		
Remedial action: Configure the IMSIattribute of the class SubscriberTrace and perform the call trace recording session.Verify the call of the IMSI to be traced.Verify the subscriber record files that are uploaded to the SFTP server defined by the attributes sftpServer and rootDirectoryof a class SubscriberTraceConfig.		

Table 23-43 BSR_agpsServiceUnavailable

Alarm	Attributes	Applicable major release
Name: BSR_agpsServiceUnavailable (5803) Type: processingErrorAlarm Package: femto.BSR_agpsServiceUnavailable Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised if the AGPS Service is unavailable		
Remedial action: The alarm will clear automatically when the AGPS server becomes available. If the problem persists, contact Nokia customer support.		

Table 23-44 BSR_allReservedFemtoCellsInUse

Alarm	Attributes	Applicable major release
Name: BSR_allReservedFemtoCellsInUse (5804) Type: operationalViolation Package: femto.BSR_allReservedFemtoCellsInUse Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2
Description: Neighbour determination mechanisms have discovered that all Femto reserved scrambling codes in the neighbourhood of the H-BSR are in use. This is due to Insufficient reserved PSC for the deployment scenario.		
Remedial action: The operator could increase number of reserved Small Cell PSCs. The alarm will clear automatically when the PSC becomes available. If the problem persists, contact Nokia customer support		

Table 23-45 BSR_applicationInsane

Alarm	Attributes	Applicable major release
Name: BSR_applicationInsane (5805) Type: processingErrorAlarm Package: femto.BSR_applicationInsane Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareProgramError	Release: • 14.2
Description: Application software is not functioning properly. - This is raised for persistent audit failures.		
Remedial action: The alarm will be cleared when audit no longer detects a problem. If the problem persists, contact Nokia customer support		

Table 23-46 BSR_autoconfigfailure

Alarm	Attributes	Applicable major release
Name: BSR_autoconfigfailure (5806) Type: operationalViolation Package: femto.BSR_autoconfigfailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: Auto-configuration failure.		
Remedial action: The alarm will be cleared when the autoconfiguratio succeeds. If the problem persists, contact Nokia customer support.		

Table 23-47 BSR_basebandReconfigfailed

Alarm	Attributes	Applicable major release
Name: BSR_basebandReconfigfailed (5808) Type: processingErrorAlarm Package: femto.BSR_basebandReconfigfailed Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Reconfiguration of the baseband array is failed.		
Remedial action: The fault will be cleared automatically when the Small Cell restarts.. Restart the re-configuration of the 3G Network Listening for the Small Cell. If the problem persists, contact Nokia customer support.		

Table 23-48 BSR_bCHGuardTimeExpired

Alarm	Attributes	Applicable major release
Name: BSR_bCHGuardTimeExpired (5807) Type: processingErrorAlarm Package: femto.BSR_bCHGuardTimeExpired Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: BCH Decode guard timer has expired.		
Remedial action: No operator intervention is required.		

Table 23-49 BSR_bsrIdClash

Alarm	Attributes	Applicable major release
Name: BSR_bsrIdClash (5809) Type: operationalViolation Package: femto.BSR_bsrIdClash Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is generated when the BSR-Id is already used by another BSR.		
Remedial action: Use a different Small Cell Identifier. If the problem persists or for help on the identifier, contact Nokia customer support		

Table 23-50 BSR_cellBroadcastOverload

Alarm	Attributes	Applicable major release
Name: BSR_cellBroadcastOverload (5810) Type: qualityOfServiceAlarm Package: femto.BSR_cellBroadcastOverload Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 14.2

Table 23-50 BSR_cellBroadcastOverload (continued)

Alarm	Attributes	Applicable major release
Description: This fault is raised when CBS messages are rejected due to CBS Admission Control.		
Remedial action: This alarm will be cleared when the subsequent CBS message passes the Admission control		

Table 23-51 BSR_cellSearchGuardTimeExpired

Alarm	Attributes	Applicable major release
Name: BSR_cellSearchGuardTimeExpired (5811) Type: processingErrorAlarm Package: femto.BSR_cellSearchGuardTimeExpired Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Cell Search function guard timer has expired.		
Remedial action: No operator intervention is required.		

Table 23-52 BSR_conflictingCIO

Alarm	Attributes	Applicable major release
Name: BSR_conflictingCIO (5812) Type: processingErrorAlarm Package: femto.BSR_conflictingCIO Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when there are multiple neighbour cells which cannot be uniquely identified in UE measurement reports for which different values of Cell Individual Offset will be applied. This shall apply for 3G neighbour cells when there is ARFCN/PSC reuse and 2G neighbour cells where there is ARFCN reuse without BSIC used to identify the cell.This warning shall be automatically cleared when conflicting CIO condition no longer exists.		
Remedial action: No operator intervention required, but alarm will be cleared automatically when conflicting CIO condition no longer exists.		

Table 23-53 BSR_conflictingQoffset

Alarm	Attributes	Applicable major release
Name: BSR_conflictingQoffset (5813) Type: processingErrorAlarm Package: femto.BSR_conflictingQoffset Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when there are multiple neighbour cells which cannot be uniquely identified for which different values of Qoffset have been configured. This shall apply for 3G neighbour cells when there is ARFCN/PSC reuse.This warning shall be automatically cleared when conflicting offset condition no longer exists.		

Table 23-53 BSR_conflictingQoffset (continued)

Alarm	Attributes	Applicable major release
Remedial action: No operator intervention required, but alarm will be cleared automatically when conflicting offset condition no longer exists.		

Table 23-54 BSR_constraintsCheckFailure

Alarm	Attributes	Applicable major release
Name: BSR_constraintsCheckFailure (8470) Type: processingErrorAlarm Package: femto.BSR_constraintsCheckFailure Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when there is one or more constraints failure at BSR start-up. Even though this fault is raised, Femto may offer service. The fault shall be cleared if all the constraints pass later which may be due to online modification of parameters.		
Remedial action: Identify the constraints that fail. Modify the value of the parameters to satisfy the constraints		

Table 23-55 BSR_creationOfSecondSAFailed

Alarm	Attributes	Applicable major release
Name: BSR_creationOfSecondSAFailed (5814) Type: operationalViolation Package: femto.BSR_creationOfSecondSAFailed Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The creation of the second Child SA on 1st IPsec tunnel failed. Femto BSR goes to disabled/degraded state. This fault can be cleared by a local or remote Femto BSR reset or if the IPsec tunnel #1 will be established during a fault handling procedure; i.e. handling of IPsec Tunnel down.		
Remedial action: No operator intervention is required.		

Table 23-56 BSR_detectedCollapsingLAI

Alarm	Attributes	Applicable major release
Name: BSR_detectedCollapsingLAI (5815) Type: processingErrorAlarm Package: femto.BSR_detectedCollapsingLAI Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: LAI value conflicts with another one in use already.		
Remedial action: The operator should reconfigure the LAC on one of conflicting BSRs as described in the additional text associated with the alarm. If the problem persists, contact Nokia customer support.		

Table 23-57 BSR_deviceAuthenticationFailure

Alarm	Attributes	Applicable major release
Name: BSR_deviceAuthenticationFailure (5816) Type: securityServiceOrMechanismViolation Package: femto.BSR_deviceAuthenticationFailure Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: authenticationFailure	Release: • 14.2
Description: This fault is raised if device authentication fails.		
Remedial action: Contact Nokia customer support for help in resolving the authentication issue. The alarm will be cleared automatically when the authentication of the Small Cell is successful.		

Table 23-58 BSR_downloadSwDiffThanTargetSw

Alarm	Attributes	Applicable major release
Name: BSR_downloadSwDiffThanTargetSw (12397) Type: processingErrorAlarm Package: femto.BSR_downloadSwDiffThanTargetSw Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when AP receives the TR-069 download command and identifies that the target SW image URL is different than the already downloaded SW image URL.		
Remedial action: Operator needs to ensure that the software image version in Step 1 and Step 2 of Two Step Upgrade Feature (227490) is same.		

Table 23-59 BSR_frequencyOutOfSync

Alarm	Attributes	Applicable major release
Name: BSR_frequencyOutOfSync (5817) Type: equipmentAlarm Package: femto.BSR_frequencyOutOfSync Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSynchronisation	Release: • 14.2
Description: Alarm triggered when frequency goes out of sync		
Remedial action: NA		

Table 23-60 BSR_gatewayConnectivityProblemsStandbyNode

Alarm	Attributes	Applicable major release
Name: BSR_ gatewayConnectivityProblemsStandbyNode (5819) Type: operationalViolation Package: femto.BSR_ gatewayConnectivityProblemsStandbyNode Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if the number of times the connection to the standby node has been dropped exceeds the defined threshold over the PM granularity period.		
Remedial action: Check the standby SCGW IP address and connectivity.		

Table 23-61 BSR_gatewayConnectivityProblemsStandyNode

Alarm	Attributes	Applicable major release
Name: BSR_ gatewayConnectivityProblemsStandyNode (5820) Type: operationalViolation Package: femto.BSR_ gatewayConnectivityProblemsStandyNode Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if the number of times the connection to the standby node has been dropped exceeds the defined threshold over the PM granularity period.		
Remedial action: NA		

Table 23-62 BSR_gGSNselectionFailure

Alarm	Attributes	Applicable major release
Name: BSR_gGSNselectionFailure (5818) Type: processingErrorAlarm Package: femto.BSR_gGSNselectionFailure Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised if PDP Context Activation attempt by UE that received GGSN selection support resulted in a PDP Context Rejection by the SGSN. Likely invalid Replacement APN configured in attribute BSR::gGSNselectionReplacementAPN.		
Remedial action: Check the Replacement APN configured in the attribute BSR::gGSNselectionReplacementAPN. If the problem persists, contact Nokia customer support.		

Table 23-63 BSR_gsmBandNotSupported

Alarm	Attributes	Applicable major release
Name: BSR_gsmBandNotSupported (5822) Type: equipmentAlarm Package: femto.BSR_gsmBandNotSupported Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Hardware is not compatible with the gsm band configured.		
Remedial action: The operator should configure the supported bands or set the parameter gsmListenerPicoBasedEnabled to false. If the problem persists, contact Nokia customer support		

Table 23-64 BSR_gsmBCCHDecodeGuardTimerExpired

Alarm	Attributes	Applicable major release
Name: BSR_gsmBCCHDecodeGuardTimerExpired (5821) Type: processingErrorAlarm Package: femto.BSR_ gsmBCCHDecodeGuardTimerExpired Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: BCCH Decode guard timer has expired for 2G Network Listening (Baseband based).		
Remedial action: No operator intervention is required.		

Table 23-65 BSR_gsmCellSearchGuardTimerExpired

Alarm	Attributes	Applicable major release
Name: BSR_gsmCellSearchGuardTimerExpired (5823) Type: processingErrorAlarm Package: femto.BSR_ gsmCellSearchGuardTimerExpired Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Cell Search function guard timer has expired for 2G Network Listening (Baseband based).		
Remedial action: No operator intervention is required.		

Table 23-66 BSR_gsmThresholdCriteriaNotMet

Alarm	Attributes	Applicable major release
Name: BSR_gsmThresholdCriteriaNotMet (5824) Type: processingErrorAlarm Package: femto.BSR_gsmThresholdCriteriaNotMet Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The threshold criteria for detection of gsm cells has not been met and this has resulted in an open search for more cells.		
Remedial action: The operator could change threshold criteria MIM Parameters		

Table 23-67 BSR_gTPULocalPortWCDMAFailure

Alarm	Attributes	Applicable major release
Name: BSR_gTPULocalPortWCDMAFailure (8169) Type: communicationsAlarm Package: femto.BSR_gTPULocalPortWCDMAFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is sent when the MS-MCI AP fails to use the local GTP-U port defined by attribute BSR:gTPULocalPortWCDMA.		
Remedial action: Operator could check configuration of attribute BSR:gTPULocalPortWCDMA		

Table 23-68 BSR_hostingPartyAuthenticationFailure

Alarm	Attributes	Applicable major release
Name: BSR_hostingPartyAuthenticationFailure (5825) Type: securityServiceOrMechanismViolation Package: femto.BSR_ hostingPartyAuthenticationFailure Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: authenticationFailure	Release: • 14.2
Description: This fault is raised if hosting party authentication fails.		
Remedial action: The alarm will clear automatically when the hosting party authentication is successful. If the problem persists, contact Nokia customer support.		

Table 23-69 BSR_hsimNotPresent

Alarm	Attributes	Applicable major release
Name: BSR_hsimNotPresent (5826) Type: securityServiceOrMechanismViolation Package: femto.BSR_hsimNotPresent Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: otherSecurityService	Release: • 14.2

Table 23-69 BSR_hsimNotPresent (continued)

Alarm	Attributes	Applicable major release
Description: This fault is raised if no HSIM is present on the UICC and the SecGW requires Hosting Party authentication.		
Remedial action: Contact Nokia customer support for help		

Table 23-70 BSR_invalidDatabaseDetected

Alarm	Attributes	Applicable major release
Name: BSR_invalidDatabaseDetected (5827) Type: operationalViolation Package: femto.BSR_invalidDatabaseDetected Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The BSR detects an invalid database e.g. due to a consistency error.		
Remedial action: Fix the provisioning errors		

Table 23-71 BSR_invalidMocnConfiguration

Alarm	Attributes	Applicable major release
Name: BSR_invalidMocnConfiguration (5828) Type: operationalViolation Package: femto.BSR_invalidMocnConfiguration Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when default operator is not configured when required to select MOCN operator for nonsupporting UE.Alarm data shall include 'Neighbour cells not found' when mocnOperatorSelection is set to 'macroPLMN' and macro cellsare not detected and default MOCN operator is not configured.		
Remedial action: Operator is required to configure default MOCN operator in BSR::defaultMocnOperatorRef		

Table 23-72 BSR_ipsecConfigurationAlarm

Alarm	Attributes	Applicable major release
Name: BSR_ipsecConfigurationAlarm (5829) Type: operationalViolation Package: femto.BSR_ipsecConfigurationAlarm Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The Femto BSR detected a SW-incompatibility on IPsec Router for the requested IPsec configuration. Femto BSR goes to disabled/degraded state. This fault can be cleared by a local or remote Femto BSR reset or if the IPsec tunnel #1 will be established during a fault handling procedure; i.e. handling of IPsec Tunnel down.		

Table 23-72 BSR_ipsecConfigurationAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Operator could update the Ipsec router to support the second SA feature or disable the feature on BSR (enableTwoSA="false"		

Table 23-73 BSR_ipsecTunnelAlarm

Alarm	Attributes	Applicable major release
Name: BSR_ipsecTunnelAlarm (5830) Type: operationalViolation Package: femto.BSR_ipsecTunnelAlarm Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The establishment of 2nd IPSec tunnel failed.or 2nd IPsec tunnel goes down. Femto BSR goes to disabled/failed state but OA and M is still active. This fault can be cleared after a successful tunnel establishment during a fault handling procedure.		
Remedial action: Operator should check configuration of the 2nd (high priority) tunnel and the network or disable the two Ipsec tunnels feature (enableTwoIpsecTunnels="false)."		

Table 23-74 BSR_ipsecTunnelFailureNoResponse

Alarm	Attributes	Applicable major release
Name: BSR_ipsecTunnelFailureNoResponse (5831) Type: communicationsAlarm Package: femto.BSR_ipsecTunnelFailureNoResponse Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: This fault is raised if the Femto BSR did not receive a response to IKE_INIT or IKE_AUTH, if Dead Peer Detection (DPD) encountered an unresponsive SeGW, or if the Femto BSR could not resolve the SeGW FQDN to an IP address (when/if FQDN was used).		
Remedial action: For standalone AP, this is because of SA_INIT failure or DNS lookup failure. Check network connectivity.		

Table 23-75 BSR_ipsecTunnelFailureUnknownCause

Alarm	Attributes	Applicable major release
Name: BSR_ipsecTunnelFailureUnknownCause (5832) Type: processingErrorAlarm Package: femto.BSR_ipsecTunnelFailureUnknownCause Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault indicates a failure to connect to the SeGW which could not be classified. It is used only if none of the more specific error types is suitable. Additional alarm text could be provided to qualify the fault.		

Table 23-75 BSR_ipsecTunnelFailureUnknownCause (continued)

Alarm	Attributes	Applicable major release
Remedial action: For MSAP this error occurs if there is a SA_INIT failure response. Check network connectivity.		

Table 23-76 BSR_isolatedCellOverlapped

Alarm	Attributes	Applicable major release
Name: BSR_isolatedCellOverlapped (5833) Type: processingErrorAlarm Package: femto.BSR_isolatedCellOverlapped Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: If the isolated cell detects any other isolated cells or Femtos, this fault is raised to indicate an overlap with at least another cell.		
Remedial action: No operator intervention is required. The alarm will be cleared by the Small Cell when the overlap is resolved. If the problem persists, contact Nokia customer support.		

Table 23-77 BSR_lmcFailure

Alarm	Attributes	Applicable major release
Name: BSR_lmcFailure (5834) Type: equipmentAlarm Package: femto.BSR_lmcFailure Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: This fault is created when either or all of the Location, Movement and National Location Lock check failed.		
Remedial action: The Small Cell MO is disabled. Check that the Small Cell is in correct location. Use MIM parameters to determine the failed tests and change the various parameters to relax the criteria or disable the test. If the problem persists, contact Nokia customer support.		

Table 23-78 BSR_lossOfSyncSourceGps

Alarm	Attributes	Applicable major release
Name: BSR_lossOfSyncSourceGps (5835) Type: equipmentAlarm Package: femto.BSR_lossOfSyncSourceGps Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: synchronizationSourceMis-match	Release: • 14.2
Description: Alarm triggered when sync source is lost via GPS		
Remedial action: NA		

Table 23-79 BSR_lossOfSyncSourceNtp

Alarm	Attributes	Applicable major release
Name: BSR_lossOfSyncSourceNtp (5836) Type: equipmentAlarm Package: femto.BSR_lossOfSyncSourceNtp Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: synchronizationSourceMis-match	Release: • 14.2
Description: Alarm triggered when sync source is lost via NTP		
Remedial action: NA		

Table 23-80 BSR_lteServiceUnavailable

Alarm	Attributes	Applicable major release
Name: BSR_lteServiceUnavailable (5837) Type: qualityOfServiceAlarm Package: femto.BSR_lteServiceUnavailable Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: This fault is created when the one or more 4G subsystems have some unrecoverable error or failed.		
Remedial action: MS-MCI AP should be rebooted to clear the Alarm.		

Table 23-81 BSR_misConfigurationWarmStandby

Alarm	Attributes	Applicable major release
Name: BSR_misConfigurationWarmStandby (5838) Type: operationalViolation Package: femto.BSR_misConfigurationWarmStandby Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised if the IP addresses and warm standby feature are configured in an inconsistent fashion (e.g. using Active warm standby feature on Femto with the floating IP address configured).		
Remedial action: The alarm will be cleared by the Small Cell when the configuration is correct. If the problem persists, contact Nokia customer support.		

Table 23-82 BSR_missedTriggeringSelfOpt

Alarm	Attributes	Applicable major release
Name: BSR_missedTriggeringSelfOpt (11140) Type: processingErrorAlarm Package: femto.BSR_missedTriggeringSelfOpt Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when the AP fails to run self optimization in the last 24 hours.		
Remedial action: If the service level KPIs are degraded, trigger an on-demand self-optimation to clear the alarm. Check if the self-optimzation schedule is running appropriately for the AP.		

Table 23-83 BSR_mnoDataUpdateFailure

Alarm	Attributes	Applicable major release
Name: BSR_mnoDataUpdateFailure (11141) Type: operationalViolation Package: femto.BSR_mnoDataUpdateFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault indicates that an MNO Data update for MS-AP or SeGW certificate update for standalone 3G was attempted and failed. Either the prospective MNO Data was not valid or there was an operational failure during an attempt to deploy the data.		
Remedial action: Root cause isolate the problem and resolve, then repeat the procedure.		

Table 23-84 BSR_msAPoutOfMemory

Alarm	Attributes	Applicable major release
Name: BSR_msAPoutOfMemory (11142) Type: processingErrorAlarm Package: femto.BSR_msAPoutOfMemory Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfMemory	Release: • 14.2
Description: MSAP has run out memory. It could be either RAM or disk space.		
Remedial action: MS AP could be running on low memory. If the service level KPIs are degraded, reboot the AP.		

Table 23-85 BSR_noCarrierSelected

Alarm	Attributes	Applicable major release
Name: BSR_noCarrierSelected (5839) Type: operationalViolation Package: femto.BSR_noCarrierSelected Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The fault is raised when no carrier for the FBSR can be selected under different situations, which are detailed in AdditionalText.		
Remedial action: ReConfigure the candidate list of carriers and other parameters		

Table 23-86 BSR_noMacroCellFound

Alarm	Attributes	Applicable major release
Name: BSR_noMacroCellFound (5840) Type: processingErrorAlarm Package: femto.BSR_noMacroCellFound Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if no macro cells were found and dynamic LAC-SAC is enabled and there is no previsioning to fallback on.		
Remedial action: This fault is raised if no macro cells were found and dynamic LAC-SAC is enabled and there is no previsioning to fallback on.		

Table 23-87 BSR_ntpDrift

Alarm	Attributes	Applicable major release
Name: BSR_ntpDrift (5841) Type: equipmentAlarm Package: femto.BSR_ntpDrift Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised when either forward or backward NTP drift is greater than one minute.		
Remedial action: Adjust the NTP drift.		

Table 23-88 BSR_pwdLoginFailure

Alarm	Attributes	Applicable major release
Name: BSR_pwdLoginFailure (12739) Type: operationalViolation Package: femto.BSR_pwdLoginFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Indicates Account lockdown after maximum number of unsuccessful login attempts. The type of account locked is explained in additional text.		
Remedial action: Password reset procedure should be triggered to enable the account again on which the alarm will be cleared.		

Table 23-89 BSR_pwdNokiaSupportAccountOperationFailure

Alarm	Attributes	Applicable major release
Name: BSR_ pwdNokiaSupportAccountOperationFailure (12740) Type: operationalViolation Package: femto.BSR_ pwdNokiaSupportAccountOperationFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Indicates a failure in password login account operation like creation/update/deletion of Nokia Support team account. The details of failure are available in additional text field.		
Remedial action: Identify the root cause based on the failure description and take appropriate action. Repeat the procedure again.		

Table 23-90 BSR_pwdNokiaSupportLoginFailure

Alarm	Attributes	Applicable major release
Name: BSR_pwdNokiaSupportLoginFailure (12967) Type: operationalViolation Package: femto.BSR_pwdNokiaSupportLoginFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Indicates Nokia Support Account lockdown after maximum number of unsuccessful login attempts.		
Remedial action: Password reset procedure should be triggered to enable the Nokia support account again.		

Table 23-91 BSR_pwdServiceProviderAccountOperationFailure

Alarm	Attributes	Applicable major release
Name: BSR_ pwdServiceProviderAccountOperationFailure (12741) Type: operationalViolation Package: femto.BSR_ pwdServiceProviderAccountOperationFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Indicates a failure in password login account operation like creation/update/deletion of Service Provider account. The details of failure are available in additional text field.		
Remedial action: Identify the root cause based on the failure description and take appropriate action. Repeat the procedure again.		

Table 23-92 BSR_pwdServiceProviderLoginFailure

Alarm	Attributes	Applicable major release
Name: BSR_pwdServiceProviderLoginFailure (12968) Type: operationalViolation Package: femto.BSR_pwdServiceProviderLoginFailure Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Indicates Service Provider Account lockdown after maximum number of unsuccessful login attempts.		
Remedial action: Password reset procedure should be triggered to enable the service provider account again.		

Table 23-93 BSR_queueOverload

Alarm	Attributes	Applicable major release
Name: BSR_queueOverload (5842) Type: qualityOfServiceAlarm Package: femto.BSR_queueOverload Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 14.2
Description: This is reported when no free paging occasion is found for scheduling a paging record.		
Remedial action: The alarm will be cleared by the Small Cell when the paging queue is freed up. If the problem persists, contact Nokia customer support.		

Table 23-94 BSR_resetCompleted

Alarm	Attributes	Applicable major release
Name: BSR_resetCompleted (5843) Type: processingErrorAlarm Package: femto.BSR_resetCompleted Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is generated when a reset was successfully performed and BSR is 'stable' for a certain time after the reset.		
Remedial action: No operator intervention is required		

Table 23-95 BSR_resetFailed

Alarm	Attributes	Applicable major release
Name: BSR_resetFailed (5844) Type: processingErrorAlarm Package: femto.BSR_resetFailed Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is generated when the reset action is failed by platform.		
Remedial action: No operator intervention is required		

Table 23-96 BSR_resetInitiated

Alarm	Attributes	Applicable major release
Name: BSR_resetInitiated (5845) Type: processingErrorAlarm Package: femto.BSR_resetInitiated Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is generated short before the BSR resets (reset will be delayed for a few seconds). It contains the reset cause 'manually initiated' or 'autonomously initiated'.		
Remedial action: No operator intervention is required		

Table 23-97 BSR_sameLaRaMacroAutoConfigFail

Alarm	Attributes	Applicable major release
Name: BSR_sameLaRaMacroAutoConfigFail (5846) Type: operationalViolation Package: femto.BSR_sameLaRaMacroAutoConfigFail Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if the same LAC/RAC Macro auto configuration fails, but the BSR Femto remains in service.		

Table 23-97 BSR_sameLaRaMacroAutoConfigFail (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm will be cleared by the Small Cell when the auto-configuration succeeds. If the problem persists, contact Nokia customer support		

Table 23-98 BSR_sameLaRaMacroAutoConfigFailOutOfService

Alarm	Attributes	Applicable major release
Name: BSR_ sameLaRaMacroAutoConfigFailOutOfService (5847) Type: operationalViolation Package: femto.BSR_ sameLaRaMacroAutoConfigFailOutOfService Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised if the Femto BSR has been configured to set its LAC/RAC from the macro cell and the BSR cannot find one and results in the BSR Femto being taken out of service.		
Remedial action: The fault will be cleared automatically when the Small Cell finds a macro cell from which to set its LAC/RAC. If the problem persists, contact Nokia customer support.		

Table 23-99 BSR_scepInvalidConfiguration

Alarm	Attributes	Applicable major release
Name: BSR_scepInvalidConfiguration (11143) Type: integrityViolation Package: femto.BSR_scepInvalidConfiguration Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: informationMissing	Release: • 14.2
Description: This fault indicates that the SCEP protocol is enabled for use but one or more provisioned or configured parameters are missing, incorrect, incomplete, or inconsistent.		
Remedial action: Determine whether configured or provisioned parameter is involved. Make correction to parameter and activate with corrected parameter.		

Table 23-100 BSR_scepProtocolError

Alarm	Attributes	Applicable major release
Name: BSR_scepProtocolError (11144) Type: operationalViolation Package: femto.BSR_scepProtocolError Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • 14.2
Description: This fault indicates that an SCEP protocol error was detected.		
Remedial action: Check configuration of protocol engine on both client and server side to RCA interop issue.		

Table 23-101 BSR_scepProvisionedCertMismatch

Alarm	Attributes	Applicable major release
Name: BSR_scepProvisionedCertMismatch (11145) Type: integrityViolation Package: femto.BSR_scepProvisionedCertMismatch Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: informationModificationDetected	Release: • 14.2
Description: This fault indicates that the operational certificates were compared with the operator CMS provided certificates and these certificates do not match.		
Remedial action: Check each certificate, update the incorrect instance, RCA to determine how mismatch occurred.		

Table 23-102 BSR_securityViolation

Alarm	Attributes	Applicable major release
Name: BSR_securityViolation (5848) Type: securityServiceOrMechanismViolation Package: femto.BSR_securityViolation Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unauthorizedAccessAttempt	Release: • 14.2
Description: This fault is created when the BSR-OAM detects an un-authorised interface access of BSR.		
Remedial action: Investigate the security violation. The fault will be cleared automatically when the Small Cell is reset. If the problem persists, contact Nokia customer support		

Table 23-103 BSR_selfoptNotRun

Alarm	Attributes	Applicable major release
Name: BSR_selfoptNotRun (5849) Type: operationalViolation Package: femto.BSR_selfoptNotRun Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 14.2
Description: Self optimization has not been run during the quiet period allotted as active calls present.		
Remedial action: The alarm will be cleared by the Small Cell next time the self optimization runs. If the problem persists, contact Nokia customer support		

Table 23-104 BSR_softwareCompatibilityError

Alarm	Attributes	Applicable major release
Name: BSR_softwareCompatibilityError (5850) Type: processingErrorAlarm Package: femto.BSR_softwareCompatibilityError Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: BSR has received an Error Indication in BSRAP protocol.		
Remedial action: Ensure that all the femtos in one group operate in same software version		

Table 23-105 BSR_spareBSRAlarm1

Alarm	Attributes	Applicable major release
Name: BSR_spareBSRAlarm1 (8170) Type: processingErrorAlarm Package: femto.BSR_spareBSRAlarm1 Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-106 BSR_spareBSRAlarm2

Alarm	Attributes	Applicable major release
Name: BSR_spareBSRAlarm2 (8171) Type: processingErrorAlarm Package: femto.BSR_spareBSRAlarm2 Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-107 BSR_spareBSRAlarm3

Alarm	Attributes	Applicable major release
Name: BSR_spareBSRAlarm3 (8172) Type: processingErrorAlarm Package: femto.BSR_spareBSRAlarm3 Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-108 BSR_systemOverload

Alarm	Attributes	Applicable major release
Name: BSR_systemOverload (5851) Type: qualityOfServiceAlarm Package: femto.BSR_systemOverload Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 14.2
Description: This fault is raised for CPU overload and Memory overload.		
Remedial action: The alarm will be cleared by the Small Cell when the overload clears. If the problem persists, contact Nokia customer support.		

Table 23-109 BSR_tamperDetected

Alarm	Attributes	Applicable major release
Name: BSR_tamperDetected (5852) Type: securityServiceOrMechanismViolation Package: femto.BSR_tamperDetected Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unauthorizedAccessAttempt	Release: • 14.2
Description: This fault is raised if tampering access has been detected by the Femto BSR.		
Remedial action: Contact Nokia customer support for help in clearing the tamperDetected alarm		

Table 23-110 BSR_thresholdCriteriaNotMet

Alarm	Attributes	Applicable major release
Name: BSR_thresholdCriteriaNotMet (5853) Type: processingErrorAlarm Package: femto.BSR_thresholdCriteriaNotMet Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The threshold criteria for detection of cells has not been met and this has resulted in an open search for more cells.		
Remedial action: The operator could reconfigure the threshold criteria MIM Parameters (macroCellRSCPthreshold, macroCellEcNo-Threshold, RatioMacroCellbelowThreshold). If the problem persists, contact Nokia customer support.		

Table 23-111 BSR_timeOutOfSync

Alarm	Attributes	Applicable major release
Name: BSR_timeOutOfSync (5854) Type: equipmentAlarm Package: femto.BSR_timeOutOfSync Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSynchronisation	Release: • 14.2
Description: Alarm triggered when time goes out of sync as a result of failing to synchronize with timing source.		

Table 23-111 BSR_timeOutOfSync (continued)

Alarm	Attributes	Applicable major release
Remedial action: NA		

Table 23-112 BSR_txPowerConfigurationWarning

Alarm	Attributes	Applicable major release
Name: BSR_txPowerConfigurationWarning (5855) Type: qualityOfServiceAlarm Package: femto.BSR_txPowerConfigurationWarning Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: This fault is raised if a BSR spends greater than thrJCOOverload percent of time at reduced power output.		
Remedial action: This alarm is cleared if a subsequent PM reporting period has a percentage of time spent in a reduced Tx Power state less thanthrJCOOverload		

Table 23-113 BSR_txPowerLimitReached

Alarm	Attributes	Applicable major release
Name: BSR_txPowerLimitReached (5856) Type: qualityOfServiceAlarm Package: femto.BSR_txPowerLimitReached Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: This fault is raised if a BSR calculates that a power change required as part of JCO algorithm would make the Femto operate outside of its configured Tx Power limits.		
Remedial action: This alarm shall be cleared when the transaction associated with this power change is either rejected or revoked.		

Table 23-114 BSR_umtsBandNotSupported

Alarm	Attributes	Applicable major release
Name: BSR_umtsBandNotSupported (5857) Type: equipmentAlarm Package: femto.BSR_umtsBandNotSupported Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Hardware is not compatible with the umts band configured.		
Remedial action: The operator should configure the supported UMTS bands. If the problem persists, contact Nokia customer support		

Table 23-115 BSR_unknownTimeOfDay

Alarm	Attributes	Applicable major release
Name: BSR_unknownTimeOfDay (5858) Type: processingErrorAlarm Package: femto.BSR_unknownTimeOfDay Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if following a reset the FemtoBSR is able to establish a connection to the Mobile Operator's network but is unable to set the time of day from the SNTP server. It is also raised if the FemtoBSR is able to set the time of day, but is subsequently unable to update it from the SNTP server for a period of 7 days.		
Remedial action: Check to see if the SNTP Server is reachable from the Femto via tunnel.		

Table 23-116 BSR_unsecureTimeOfDay

Alarm	Attributes	Applicable major release
Name: BSR_unsecureTimeOfDay (8471) Type: timeDomainViolation Package: femto.BSR_unsecureTimeOfDay Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: otherSecurityService	Release: • 14.2
Description: Time Of Day offered by the active timing reference source (such as GPS or NTP or PTP) is different than the time of day read from network's secure SNTP/PTP server.		
Remedial action: Operator should check phase reference sources (GPS or PTP (future)) for possible incorrect time spoofing or other incorrect behavior.		

Table 23-117 BSR_wcdmaServiceUnavailable

Alarm	Attributes	Applicable major release
Name: BSR_wcdmaServiceUnavailable (5859) Type: qualityOfServiceAlarm Package: femto.BSR_wcdmaServiceUnavailable Raised on class: femto.Femto	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: This fault is created when the one or more 3G subsystems have some unrecoverable error or failed.		
Remedial action: The alarm will clear automatically when the MS-MCI AP is rebooted. If the operating Mode is wcdmaAndLTE, LTE service could be operational, so MS-MCI AP should be rebooted with least impact to service.		

Table 23-118 bulkoperationresultOverload

Alarm	Attributes	Applicable major release
Name: bulkoperationresultOverload (11167) Type: equipmentAlarm Package: femto.bulkoperationresultOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for bulk operation result events.		
Remedial action: Threshold exceeds for bulk operation result events		

Table 23-119 CECTL_layer1CommunicationFailure

Alarm	Attributes	Applicable major release
Name: CECTL_layer1CommunicationFailure (5881) Type: equipmentAlarm Package: femto.CECTL_layer1CommunicationFailure Raised on class: femto.CECTL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Layer1 fails to respond.		
Remedial action: The alarm will clear automatically when the MS-MCI AP is rebooted.If the problem persists, contact Nokia customer support.		

Table 23-120 CECTL_layerOneResetFailure

Alarm	Attributes	Applicable major release
Name: CECTL_layerOneResetFailure (5882) Type: equipmentAlarm Package: femto.CECTL_layerOneResetFailure Raised on class: femto.CECTL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Reset of layer one failed.		
Remedial action: The MSAP automatically reset when the alarm is triggered. If this alarm persists, reset the MSAP. If the problem persists, contact Nokia customer support.		

Table 23-121 CECTL_picoArrayCommunicationFailure

Alarm	Attributes	Applicable major release
Name: CECTL_picoArrayCommunicationFailure (5883) Type: equipmentAlarm Package: femto.CECTL_ picoArrayCommunicationFailure Raised on class: femto.CECTL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2

Table 23-121 CECTL_picoArrayCommunicationFailure (continued)

Alarm	Attributes	Applicable major release
Description: Picoarray fails to respond.		
Remedial action: NA		

Table 23-122 CertificateEnrollment_certificateEnrollmentFailure

Alarm	Attributes	Applicable major release
Name: CertificateEnrollment_ certificateEnrollmentFailure (8174) Type: processingErrorAlarm Package: femto.CertificateEnrollment_ certificateEnrollmentFailure Raised on class: femto.CertificateEnrollment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: CMPv2 enrolment to operator PKI failed		
Remedial action: Contact Nokia customer support for help inidentifying the problem		

Table 23-123 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 14.2
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 23-124 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 14.2
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		

Table 23-124 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 23-125 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministratively Down	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 23-126 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 23-127 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 23-128 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 14.2
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 23-129 cpeauthactiveconnectionscurrentcount

Alarm	Attributes	Applicable major release
Name: cpeauthactiveconnectionscurrentcount (6274) Type: equipmentAlarm Package: femto.cpeauthactiveconnectionscurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication Active Connections Current Count		
Remedial action: Not available		

Table 23-130 cpeauthactiveconnectionshighcount

Alarm	Attributes	Applicable major release
Name: cpeauthactiveconnectionshighcount (6275) Type: equipmentAlarm Package: femto.cpeauthactiveconnectionshighcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication Active Connections High Count		
Remedial action: Not available		

Table 23-131 cpeauthcurrcapacity

Alarm	Attributes	Applicable major release
Name: cpeauthcurrcapacity (6276) Type: equipmentAlarm Package: femto.cpeauthcurrcapacity Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication current capacity		
Remedial action: Not available		

Table 23-132 cpeauthfailedreserverequestcount

Alarm	Attributes	Applicable major release
Name: cpeauthfailedreserverequestcount (6277) Type: equipmentAlarm Package: femto.cpeauthfailedreserverequestcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication failed reserve request count		
Remedial action: Not available		

Table 23-133 cpeauthleakedconnectioncount

Alarm	Attributes	Applicable major release
Name: cpeauthleakedconnectioncount (6278) Type: equipmentAlarm Package: femto.cpeauthleakedconnectioncount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication leaked connection count		
Remedial action: Not available		

Table 23-134 cpeauthwaitingforconnectioncurrentcount

Alarm	Attributes	Applicable major release
Name: cpeauthwaitingforconnectioncurrentcount (6279) Type: equipmentAlarm Package: femto.cpeauthwaitingforconnectioncurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CPE Authentication waiting for connection count		
Remedial action: Not available		

Table 23-135 deviceactionresultOverload

Alarm	Attributes	Applicable major release
Name: deviceactionresultOverload (11168) Type: equipmentAlarm Package: femto.deviceactionresultOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for device action result events.		
Remedial action: Threshold exceeds for device action result event		

Table 23-136 devicedeletionnotificationOverload

Alarm	Attributes	Applicable major release
Name: devicedeletionnotificationOverload (11169) Type: equipmentAlarm Package: femto.devicedeletionnotificationOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for device deletion notification.		
Remedial action: Threshold exceeds for device deletion notification		

Table 23-137 deviceinformeventOverload

Alarm	Attributes	Applicable major release
Name: deviceinformeventOverload (11170) Type: equipmentAlarm Package: femto.deviceinformeventOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for device inform events.		

Table 23-137 deviceinformeventOverload (continued)

Alarm	Attributes	Applicable major release
Remedial action: Threshold exceeds for device inform events		

Table 23-138 deviceregistrationOverload

Alarm	Attributes	Applicable major release
Name: deviceregistrationOverload (11171) Type: equipmentAlarm Package: femto.deviceregistrationOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for device registration events.		
Raising condition: (('Registration Events OverLoad' EQUAL 'true'))		
Clearing condition: (('Registration Events OverLoad' EQUAL 'false'))		
Remedial action: Threshold exceeds for device registration events		

Table 23-139 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 14.2
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 23-140 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		

Table 23-140 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 23-141 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 23-142 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 14.2
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 23-143 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 14.2

Table 23-143 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 23-144 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 14.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 23-145 FemtoUpgradeRulesFileAlarm

Alarm	Attributes	Applicable major release
Name: FemtoUpgradeRulesFileAlarm (12743) Type: processingErrorAlarm Package: femto.FemtoUpgradeRulesFileAlarm Raised on class: femto.SmallCellProfileUpgradeActions	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomizationError	Release: • 14.2
Description: The alarm is raised when there is any issue with the Upgrade Rules File.		
Remedial action: Please provide a valid Femto Upgrade Rules File		

Table 23-146 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 14.2
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 23-147 functionsaddobject

Alarm	Attributes	Applicable major release
Name: functionsaddobject (6280) Type: equipmentAlarm Package: femto.functionsaddobject Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of addobject function		
Remedial action: Not available		

Table 23-148 functionsbackup

Alarm	Attributes	Applicable major release
Name: functionsbackup (6281) Type: equipmentAlarm Package: femto.functionsbackup Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of backup function		
Remedial action: Not available		

Table 23-149 functionsconfigurationdownload

Alarm	Attributes	Applicable major release
Name: functionsconfigurationdownload (6282) Type: equipmentAlarm Package: femto.functionsconfigurationdownload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2

Table 23-149 functionsconfigurationdownload (continued)

Alarm	Attributes	Applicable major release
Description: The number of configurationdownload function		
Remedial action: Not available		

Table 23-150 functionsconfigurationupload

Alarm	Attributes	Applicable major release
Name: functionsconfigurationupload (6283) Type: equipmentAlarm Package: femto.functionsconfigurationupload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of configurationupload function		
Remedial action: Not available		

Table 23-151 functionsconnect

Alarm	Attributes	Applicable major release
Name: functionsconnect (6284) Type: equipmentAlarm Package: femto.functionsconnect Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of connect function		
Remedial action: Not available		

Table 23-152 functionsdeleteobject

Alarm	Attributes	Applicable major release
Name: functionsdeleteobject (6285) Type: equipmentAlarm Package: femto.functionsdeleteobject Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of deleteobject function		
Remedial action: Not available		

Table 23-153 functionsfactoryreset

Alarm	Attributes	Applicable major release
Name: functionsfactoryreset (6286) Type: equipmentAlarm Package: femto.functionsfactoryreset Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of factoryreset function		
Remedial action: Not available		

Table 23-154 functionsfirmwareupdate

Alarm	Attributes	Applicable major release
Name: functionsfirmwareupdate (6287) Type: equipmentAlarm Package: femto.functionsfirmwareupdate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of firmwareupdate function		
Remedial action: Not available		

Table 23-155 functionsgetoptions

Alarm	Attributes	Applicable major release
Name: functionsgetoptions (6288) Type: equipmentAlarm Package: femto.functionsgetoptions Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getoptions function		
Remedial action: Not available		

Table 23-156 functionsgetparameterattributes

Alarm	Attributes	Applicable major release
Name: functionsgetparameterattributes (6289) Type: equipmentAlarm Package: femto.functionsgetparameterattributes Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getparameterattributes function		
Remedial action: Not available		

Table 23-157 functionsgetparameternames

Alarm	Attributes	Applicable major release
Name: functionsgetparameternames (6290) Type: equipmentAlarm Package: femto.functionsgetparameternames Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getparameternames function		
Remedial action: Not available		

Table 23-158 functionsgetparametervalues

Alarm	Attributes	Applicable major release
Name: functionsgetparametervalues (6291) Type: equipmentAlarm Package: femto.functionsgetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getparametervalues function		
Remedial action: Not available		

Table 23-159 functionsgetqueuedtransfers

Alarm	Attributes	Applicable major release
Name: functionsgetqueuedtransfers (6292) Type: equipmentAlarm Package: femto.functionsgetqueuedtransfers Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getqueuedtransfers function		
Remedial action: Not available		

Table 23-160 functionsgetrpcmethods

Alarm	Attributes	Applicable major release
Name: functionsgetrpcmethods (6293) Type: equipmentAlarm Package: femto.functionsgetrpcmethods Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of getrpcmethods function		
Remedial action: Not available		

Table 23-161 functionsreboot

Alarm	Attributes	Applicable major release
Name: functionsreboot (6294) Type: equipmentAlarm Package: femto.functionsreboot Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of reboot function		
Remedial action: Not available		

Table 23-162 functionsrestore

Alarm	Attributes	Applicable major release
Name: functionsrestore (6295) Type: equipmentAlarm Package: femto.functionsrestore Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of restore function		
Remedial action: Not available		

Table 23-163 functionsscheduleinform

Alarm	Attributes	Applicable major release
Name: functionsscheduleinform (6296) Type: equipmentAlarm Package: femto.functionsscheduleinform Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of scheduleinform function		
Remedial action: Not available		

Table 23-164 functionssetparameterattributes

Alarm	Attributes	Applicable major release
Name: functionssetparameterattributes (6297) Type: equipmentAlarm Package: femto.functionssetparameterattributes Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of setparameterattributes function		
Remedial action: Not available		

Table 23-165 functionssetparametervalues

Alarm	Attributes	Applicable major release
Name: functionssetparametervalues (6298) Type: equipmentAlarm Package: femto.functionssetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of setparametervalues function		
Remedial action: Not available		

Table 23-166 functionssnmpgetparametervalues

Alarm	Attributes	Applicable major release
Name: functionssnmpgetparametervalues (6299) Type: equipmentAlarm Package: femto.functionssnmpgetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of snmpgetparametervalues function		
Remedial action: Not available		

Table 23-167 functionssnmpsetparametervalues

Alarm	Attributes	Applicable major release
Name: functionssnmpsetparametervalues (6300) Type: equipmentAlarm Package: femto.functionssnmpsetparametervalues Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of snmpsetparametervalues function		
Remedial action: Not available		

Table 23-168 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 14.2
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		

Table 23-168 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 23-169 gccollectiontimeavg

Alarm	Attributes	Applicable major release
Name: gccollectiontimeavg (6301) Type: equipmentAlarm Package: femto.gccollectiontimeavg Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The average GC collection time		
Remedial action: Not available		

Table 23-170 gccount

Alarm	Attributes	Applicable major release
Name: gccount (6302) Type: equipmentAlarm Package: femto.gccount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The GC count		
Remedial action: Not available		

Table 23-171 gcfullcollectiontimeavg

Alarm	Attributes	Applicable major release
Name: gcfullcollectiontimeavg (6303) Type: equipmentAlarm Package: femto.gcfullcollectiontimeavg Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The average full GC collection time		
Remedial action: Not available		

Table 23-172 gcfullcount

Alarm	Attributes	Applicable major release
Name: gcfullcount (6304) Type: equipmentAlarm Package: femto.gcfullcount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Full GC time		
Remedial action: Not available		

Table 23-173 GPS_femtoNotInAuthorizedAreaGPS

Alarm	Attributes	Applicable major release
Name: GPS_femtoNotInAuthorizedAreaGPS (5992) Type: equipmentAlarm Package: femto.GPS_femtoNotInAuthorizedAreaGPS Raised on class: femto.GPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: Femto location detected by GPS not in the authorized location.		
Remedial action: The operator will need to disable/override the check to get BSR enabled. If the problem persists, contact Nokia customer support.		

Table 23-174 GPS_gpsHardwareFailure

Alarm	Attributes	Applicable major release
Name: GPS_gpsHardwareFailure (5993) Type: equipmentAlarm Package: femto.GPS_gpsHardwareFailure Raised on class: femto.GPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: GPS module HW Failed.		
Remedial action: Contact Nokia customer support for replacement of the GPS module		

Table 23-175 GPS_gpsLocationFailure

Alarm	Attributes	Applicable major release
Name: GPS_gpsLocationFailure (5994) Type: equipmentAlarm Package: femto.GPS_gpsLocationFailure Raised on class: femto.GPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: GPS receiver failed to return a location to the requested accuracy within the allowed duration.		

Table 23-175 GPS_gpsLocationFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm will be cleared by the Small Cell when the GPS receiver is supplying accurateinformation. If the problem persists, contact Nokia customer support		

Table 23-176 GSMListener_gsmATCmdFail

Alarm	Attributes	Applicable major release
Name: GSMListener_gsmATCmdFail (5995) Type: equipmentAlarm Package: femto.GSMListener_gsmATCmdFail Raised on class: femto.GSMListener	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: AT command has failed.		
Remedial action: The MSAP automatically reset when the alarm is triggered. If this alarm persists, reset the MSAP. If the problem persists, contact Nokia customer support.		

Table 23-177 GSMListener_gsmModuleATCmdTimeoutError

Alarm	Attributes	Applicable major release
Name: GSMListener_gsmModuleATCmdTimeoutError (5996) Type: equipmentAlarm Package: femto.GSMListener_ gsmModuleATCmdTimeoutError Raised on class: femto.GSMListener	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Failure to receive a response from an AT command.		
Remedial action: The alarm will be cleared by the Small Cell when it resets. If the problem persists, contact Nokia customer support.		

Table 23-178 GSMListener_gsmModuleFailtoInit

Alarm	Attributes	Applicable major release
Name: GSMListener_gsmModuleFailtoInit (5997) Type: equipmentAlarm Package: femto.GSMListener_gsmModuleFailtoInit Raised on class: femto.GSMListener	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: GSMListener module fails to initialize.		
Remedial action: The alarm will be cleared by the Small Cell when it resets. If the problem persists, contact Nokia customer support.		

Table 23-179 GSMListener_gsmNoCellsFound

Alarm	Attributes	Applicable major release
Name: GSMListener_gsmNoCellsFound (5998) Type: equipmentAlarm Package: femto.GSMListener_gsmNoCellsFound Raised on class: femto.GSMListener	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: No GSM cells have been found during a search.		
Remedial action: No operatorintervention is required.		

Table 23-180 hdmAlarmListenerFailure

Alarm	Attributes	Applicable major release
Name: hdmAlarmListenerFailure (6305) Type: communicationsAlarm Package: femto.hdmAlarmListenerFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This alarm indicates a communication issue with JMS Listener for Alarm notification in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-181 hdmDashboardAlarmListenerFailure

Alarm	Attributes	Applicable major release
Name: hdmDashboardAlarmListenerFailure (6306) Type: communicationsAlarm Package: femto.hdmDashboardAlarmListenerFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This alarm indicates a communication issue with JMS Listener for HDM Dashboard Alarm notification in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-182 hdmRegistrationListenerFailure

Alarm	Attributes	Applicable major release
Name: hdmRegistrationListenerFailure (6308) Type: communicationsAlarm Package: femto.hdmRegistrationListenerFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2

Table 23-182 hdmRegistrationListenerFailure (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a communication issue with JMS Listener for Registration notification in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-183 hdmReRegistrationListenerFailure

Alarm	Attributes	Applicable major release
Name: hdmReRegistrationListenerFailure (6307) Type: communicationsAlarm Package: femto.hdmReRegistrationListenerFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This alarm indicates a communication issue with JMS Listener for ReRegistration notification in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-184 hdmResynchroListenerFailure

Alarm	Attributes	Applicable major release
Name: hdmResynchroListenerFailure (6309) Type: communicationsAlarm Package: femto.hdmResynchroListenerFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This alarm indicates a communication issue with JMS Listener for ReSynch notification in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-185 hdmWebservicesFailure

Alarm	Attributes	Applicable major release
Name: hdmWebservicesFailure (6310) Type: communicationsAlarm Package: femto.hdmWebservicesFailure Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This alarm indicates a communication issue with Webservices client in SAM and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-186 hdmworkmanagercwmpservletcompletedrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagercwmpservlet-completedrequests (6311) Type: equipmentAlarm Package: femto.hdmworkmanagercwmpservletcompletedrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CWMP Servelt workmanager completed request rate		
Remedial action: Not available		

Table 23-187 hdmworkmanagercwmpservletpendingrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagercwmpservletpendingrequests (6312) Type: equipmentAlarm Package: femto.hdmworkmanagercwmpservletpendingrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM CWMP Servelt workmanager pending request count		
Remedial action: Not available		

Table 23-188 hdmworkmanagerdefaultcompletedrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagerdefaultcompletedrequests (6313) Type: equipmentAlarm Package: femto.hdmworkmanagerdefaultcompletedrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM default workmanager completed request rate		
Remedial action: Not available		

Table 23-189 hdmworkmanagerdefaultpendingrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagerdefaultpendingrequests (6314) Type: equipmentAlarm Package: femto.hdmworkmanagerdefaultpendingrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM default workmanager pending request count		
Remedial action: Not available		

Table 23-190 hdmworkmanagernbiservicecompletedrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagernbiservicecompletedrequests (6315) Type: equipmentAlarm Package: femto.hdmworkmanagernbiservicecompletedrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM NBI Service workmanager completed request rate		
Remedial action: Not available		

Table 23-191 hdmworkmanagernbiservicependingrequests

Alarm	Attributes	Applicable major release
Name: hdmworkmanagernbiservicependingrequests (6316) Type: equipmentAlarm Package: femto.hdmworkmanagernbiservicependingrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: HDM NBI workmanager pending request count		
Remedial action: Not available		

Table 23-192 healthcheckstatuscluster

Alarm	Attributes	Applicable major release
Name: healthcheckstatuscluster (12506) Type: equipmentAlarm Package: femto.healthcheckstatuscluster Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: This alarm indicates that HDM cluster is not in a healthy state. One or more managed servers could be overloaded or failed.		
Remedial action: Not available		

Table 23-193 HeNB_errorContactingBalmCalibrationServer

Alarm	Attributes	Applicable major release
Name: HeNB_errorContactingBalmCalibrationServer (11150) Type: processingErrorAlarm Package: femto.HeNB_ errorContactingBalmCalibrationServer Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is generated by SON, when the balm calibration server is unreachable and it is not cleared		
Remedial action: Fix Provision (for correct BALM v1 operation)		

Table 23-194 HeNB_errorContactingBalmThroughputSamplingServer

Alarm	Attributes	Applicable major release
Name: HeNB_ errorContactingBalmThroughputSamplingServer (11151) Type: processingErrorAlarm Package: femto.HeNB_ errorContactingBalmThroughputSamplingServer Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is generated by SON, when the balm throughput sampling server is unreachable and it is not cleared		
Remedial action: Fix Provision (for correct BALM v1 operation)		

Table 23-195 HeNB_errorCrmUnableToProvideLteuService

Alarm	Attributes	Applicable major release
Name: HeNB_errorCrmUnableToProvideLteuService (11152) Type: processingErrorAlarm Package: femto.HeNB_ errorCrmUnableToProvideLteuService Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is generated by CrM during initialization at bootup if LTEU operation is provisioned but CrM is unable to provide LTEU service, and if it is not cleared.		
Remedial action: If LTEU service is intended, make sure the correct 802.11 drivers, firmware, and hardware are installed. Check the logs (at /var/log/messages) to see if there was a configuration or Network Listen Initialization error. Provision the system correctly for the intended service.		

Table 23-196 HeNB_lteOamConfigurationFailure

Alarm	Attributes	Applicable major release
Name: HeNB_lteOamConfigurationFailure (12402) Type: processingErrorAlarm Package: femto.HeNB_lteOamConfigurationFailure Raised on class: femto.HeNB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: LTE OAM configuration failure alarm		
Remedial action: Fix provisioning accordingly		

Table 23-197 HeNB_lteOamConfigurationWarning

Alarm	Attributes	Applicable major release
Name: HeNB_lteOamConfigurationWarning (12403) Type: processingErrorAlarm Package: femto.HeNB_lteOamConfigurationWarning Raised on class: femto.HeNB	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is generated by LTE stack when it finds that the current database doesn't satisfy the constraints. . Even though this alarm is raised, Femto may offer service. The alarm shall be cleared if all the constraints pass later which may be due to online modification of parameters.		
Remedial action: Identify the constraints that fail by analysing the logs. Modify the value of the parameters to satisfy the constraints		

Table 23-198 HeNB_lteRrcSctpAssociationFailure

Alarm	Attributes	Applicable major release
Name: HeNB_lteRrcSctpAssociationFailure (12404) Type: communicationsAlarm Package: femto.HeNB_lteRrcSctpAssociationFailure Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError	Release: • 14.2
Description: RRC/SCTP association failure alarm. This alarm is triggered by: 1) eNB receives an ErrorInd from MME with Criticality Diagnostics; 2) S1Setup response timer expires and maximum retries exhausted; 3) receive S1Setup Failure from MME and maximum retries exhausted; 4) during S1Setup, SCTP conn failure; 5) SCTP s1 setup req send fails; 6) upon expiration of sctp connection recovery timer; 7) gets sctp shutdown from mme when cell is up.		
Remedial action: Depending on fault condition, the cell may need reboot to recover SCTP association. Look MME IP address in the Additional Text field of this alarm message for SCTP association.		

Table 23-199 HeNB_mmeS1SetupResponseInconsistency

Alarm	Attributes	Applicable major release
Name: HeNB_mmeS1SetupResponseInconsistency (8491) Type: processingErrorAlarm Package: femto.HeNB_ mmeS1SetupResponseInconsistency Raised on class: femto.HeNB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: All MME related to an operator (PLMN) are not reachable. PLMN that are requested to be broadcasted in SIB1 are not received in the served GUMMEI provided in S1 SETUP Responses.		
Remedial action: Fix configuration accordingly		

Table 23-200 HeNB_spareHeNBAlarm1

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm1 (8176) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm1 Raised on class: femto.HeNB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-201 HeNB_spareHeNBAlarm2

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm2 (8177) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm2 Raised on class: femto.HeNB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-202 HeNB_spareHeNBAlarm3

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm3 (8178) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm3 Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-203 HeNB_spareHeNBAlarm4

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm4 (11153) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm4 Raised on class: femto.HeNB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 4		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-204 HeNB_spareHeNBAlarm5

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm5 (11154) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm5 Raised on class: femto.HeNB	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 5		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-205 HeNB_spareHeNBAlarm6

Alarm	Attributes	Applicable major release
Name: HeNB_spareHeNBAlarm6 (11155) Type: processingErrorAlarm Package: femto.HeNB_spareHeNBAlarm6 Raised on class: femto.HeNB	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 6		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-206 httpacceptcount

Alarm	Attributes	Applicable major release
Name: httpacceptcount (6317) Type: equipmentAlarm Package: femto.httpacceptcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number if http accept		
Remedial action: Not available		

Table 23-207 httpconnectionscount

Alarm	Attributes	Applicable major release
Name: httpconnectionscount (6318) Type: equipmentAlarm Package: femto.httpconnectionscount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of http connection		
Remedial action: Not available		

Table 23-208 httpmessagessentrate

Alarm	Attributes	Applicable major release
Name: httpmessagessentrate (6319) Type: equipmentAlarm Package: femto.httpmessagessentrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The rate of http message sent		
Remedial action: Not available		

Table 23-209 httpreceivedmessagesrate

Alarm	Attributes	Applicable major release
Name: httpreceivedmessagesrate (6320) Type: equipmentAlarm Package: femto.httpreceivedmessagesrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The rate of http message reciption		
Remedial action: Not available		

Table 23-210 httpsacceptcount

Alarm	Attributes	Applicable major release
Name: httpsacceptcount (6321) Type: equipmentAlarm Package: femto.httpsacceptcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number if https accept		
Remedial action: Not available		

Table 23-211 httpsconnectionscount

Alarm	Attributes	Applicable major release
Name: httpsconnectionscount (6322) Type: equipmentAlarm Package: femto.httpsconnectionscount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of https connection		
Remedial action: Not available		

Table 23-212 httpsmessagessentrate

Alarm	Attributes	Applicable major release
Name: httpsmessagessentrate (6323) Type: equipmentAlarm Package: femto.httpsmessagessentrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The rate of https message sent		
Remedial action: Not available		

Table 23-213 httpsreceivedmessagesrate

Alarm	Attributes	Applicable major release
Name: httpsreceivedmessagesrate (6324) Type: equipmentAlarm Package: femto.httpsreceivedmessagesrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The rate of https message reciption		
Remedial action: Not available		

Table 23-214 IKESAPair_tunnelConfigFailure

Alarm	Attributes	Applicable major release
Name: IKESAPair_tunnelConfigFailure (8179) Type: communicationsAlarm Package: femto.IKESAPair_tunnelConfigFailure Raised on class: femto.IKESAPair	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: This fault is raised if the Femto BSR did not receive a response to IKE_INIT or IKE_AUTH, if Dead Peer Detection (DPD) encountered an unresponsive SeGW, or if the Femto BSR could not resolve the SeGW FQDN to an IP address (when/if FQDN was used).		
Remedial action: This alarm is applicable for MS AP and occurs when we have SA_INIT or DNS lookup fail.		

Table 23-215 informall

Alarm	Attributes	Applicable major release
Name: informall (6325) Type: equipmentAlarm Package: femto.informall Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform all		
Remedial action: Not available		

Table 23-216 informboot

Alarm	Attributes	Applicable major release
Name: informboot (6326) Type: equipmentAlarm Package: femto.informboot Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform boot		

Table 23-216 informboot (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-217 informbootstrap

Alarm	Attributes	Applicable major release
Name: informbootstrap (6327) Type: equipmentAlarm Package: femto.informbootstrap Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform bootstrap		
Remedial action: Not available		

Table 23-218 informconnectionrequest

Alarm	Attributes	Applicable major release
Name: informconnectionrequest (6328) Type: equipmentAlarm Package: femto.informconnectionrequest Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform connectionrequest		
Remedial action: Not available		

Table 23-219 informdiagnosticscomplete

Alarm	Attributes	Applicable major release
Name: informdiagnosticscomplete (6329) Type: equipmentAlarm Package: femto.informdiagnosticscomplete Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform diagnosticsComplete		
Remedial action: Not available		

Table 23-220 informdownload

Alarm	Attributes	Applicable major release
Name: informdownload (6330) Type: equipmentAlarm Package: femto.informdownload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform download		
Remedial action: Not available		

Table 23-221 informkicked

Alarm	Attributes	Applicable major release
Name: informkicked (6331) Type: equipmentAlarm Package: femto.informkicked Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform kicked		
Remedial action: Not available		

Table 23-222 informlatency

Alarm	Attributes	Applicable major release
Name: informlatency (6332) Type: equipmentAlarm Package: femto.informlatency Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform latency		
Remedial action: Not available		

Table 23-223 informlatencymax

Alarm	Attributes	Applicable major release
Name: informlatencymax (6333) Type: equipmentAlarm Package: femto.informlatencymax Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform latency.max		
Remedial action: Not available		

Table 23-224 informlatencymin

Alarm	Attributes	Applicable major release
Name: informlatencymin (6334) Type: equipmentAlarm Package: femto.informlatencymin Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform latency.min		
Remedial action: Not available		

Table 23-225 informperiodic

Alarm	Attributes	Applicable major release
Name: informperiodic (6335) Type: equipmentAlarm Package: femto.informperiodic Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform periodic		
Remedial action: Not available		

Table 23-226 informreboot

Alarm	Attributes	Applicable major release
Name: informreboot (6336) Type: equipmentAlarm Package: femto.informreboot Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform reboot		
Remedial action: Not available		

Table 23-227 informrequestdownload

Alarm	Attributes	Applicable major release
Name: informrequestdownload (6337) Type: equipmentAlarm Package: femto.informrequestdownload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform requestDownload		
Remedial action: Not available		

Table 23-228 informscheduled

Alarm	Attributes	Applicable major release
Name: informscheduled (6338) Type: equipmentAlarm Package: femto.informscheduled Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform scheduled		
Remedial action: Not available		

Table 23-229 informscheduleinform

Alarm	Attributes	Applicable major release
Name: informscheduleinform (6339) Type: equipmentAlarm Package: femto.informscheduleinform Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform scheduleInform		
Remedial action: Not available		

Table 23-230 informtransfercomplete

Alarm	Attributes	Applicable major release
Name: informtransfercomplete (6340) Type: equipmentAlarm Package: femto.informtransfercomplete Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform transferComplete		
Remedial action: Not available		

Table 23-231 informupload

Alarm	Attributes	Applicable major release
Name: informupload (6341) Type: equipmentAlarm Package: femto.informupload Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform upload		
Remedial action: Not available		

Table 23-232 informvaluechange

Alarm	Attributes	Applicable major release
Name: informvaluechange (6342) Type: equipmentAlarm Package: femto.informvaluechange Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of inform valueChange		
Remedial action: Not available		

Table 23-233 invalidloginattemptstotalcount

Alarm	Attributes	Applicable major release
Name: invalidloginattemptstotalcount (6343) Type: equipmentAlarm Package: femto.invalidloginattemptstotalcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Invalid login attempt occured on the current server		
Remedial action: Not available		

Table 23-234 ItfBGWY_itfBSGdnsFailure

Alarm	Attributes	Applicable major release
Name: ItfBGWY_itfBSGdnsFailure (6010) Type: communicationsAlarm Package: femto.ItfBGWY_itfBSGdnsFailure Raised on class: femto.ItfBGWY	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is sent when ItfBGWY link failure is detected when no response is received to DNS messages attempting to resolve the FGW FQDN. This maybe caused by timeout or a protocol error.		
Remedial action: NA		

Table 23-235 ItfBGWY_itfFGWfailure

Alarm	Attributes	Applicable major release
Name: ItfBGWY_itfFGWfailure (6012) Type: communicationsAlarm Package: femto.ItfBGWY_itfFGWfailure Raised on class: femto.ItfBGWY	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault indicates that FBSR registration in FGW is failed due to reasons other than overload.		

Table 23-235 ItfBGWY_itfFGWfailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support		

Table 23-236 ItfBGWY_itfFGWoverload

Alarm	Attributes	Applicable major release
Name: ItfBGWY_itfFGWoverload (6013) Type: equipmentAlarm Package: femto.ItfBGWY_itfFGWoverload Raised on class: femto.ItfBGWY	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: congestion	Release: • 14.2
Description: This fault indicates that FGW is overloaded and FBSR should be re-registered.		
Remedial action: The alarm will be cleared by the Small Cell when it successfully re-registers with the SCGW		

Table 23-237 ItfBGWY_itfFGWRegistrationFailure

Alarm	Attributes	Applicable major release
Name: ItfBGWY_itfFGWRegistrationFailure (6011) Type: operationalViolation Package: femto.ItfBGWY_itfFGWRegistrationFailure Raised on class: femto.ItfBGWY	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is generated when the Iu' BSR fails to register with the FGW following SCTP establishment, or update the registration for any reason other than BSR Id Clash.		
Remedial action: The alarm will be cleared by the Small Cell when it successfully re-registers with the		

Table 23-238 ItfBGWY_noResponseFromBGWY

Alarm	Attributes	Applicable major release
Name: ItfBGWY_noResponseFromBGWY (6014) Type: communicationsAlarm Package: femto.ItfBGWY_noResponseFromBGWY Raised on class: femto.ItfBGWY	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: This fault indicates that communication on the interface to BSR Gateway is interrupted. It is raised when a request from BSR application on interface to BSR Gateway timed out (typically the SCTP association is up).		
Remedial action: The alarm will be cleared by the Small Cell when the registration with BSR Gateway is successful. If the problem persists, contact Nokia customer support		

Table 23-239 ItfBPG_itfBPGdnsFailure

Alarm	Attributes	Applicable major release
Name: ItfBPG_itfBPGdnsFailure (6016) Type: communicationsAlarm Package: femto.ItfBPG_itfBPGdnsFailure Raised on class: femto.ItfBPG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is sent when ItfBPG link failure is detected when no response is received to DNS messages attempting to resolve the BPG FQDN. This maybe caused by timeout or a protocol error.		
Remedial action: The operator should check configuration of BPG FQDN. The DNS servers must be provisioned in the Small Cell. During the IPsec tunnel establishment, the DNS servers must be reachable from the Small Cell. The DNS servers must contain Resource Records for the BPG FQDN. If the problem persists, contact Nokia customer support.		

Table 23-240 ItfBPG_itfBPGLinkFailure

Alarm	Attributes	Applicable major release
Name: ItfBPG_itfBPGLinkFailure (6015) Type: communicationsAlarm Package: femto.ItfBPG_itfBPGLinkFailure Raised on class: femto.ItfBPG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: This fault is sent when ItfBPG link failure is detected when no response is received for a special DPAT procedure with version ="10 after exhausting all retries, or when no response received after 6 attempts at initialization."		
Remedial action: The alarm will be cleared by the Small Cell when the DPAT bind request succeeds. If the problem persists, contact Nokia customer support.		

Table 23-241 ItfBVG_itfBVGdnsFailure

Alarm	Attributes	Applicable major release
Name: ItfBVG_itfBVGdnsFailure (6018) Type: communicationsAlarm Package: femto.ItfBVG_itfBVGdnsFailure Raised on class: femto.ItfBVG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised when ItfBVG link failure is detected when no response is received to DNS messages attempting to resolve the BVG FQDN. This maybe caused by timeout or a protocol error.		
Remedial action: Operator could check configuration of BVG FQDN, ensure operator DNS servers are provisioned in FBSR at IPsec tunnel establishment, ensure operator DNS servers are reachable from FBSR, ensure operator DNS servers contain Resource Records for the BVG FQDN. If the problem persists, contact Nokia customer support		

Table 23-242 ItfBVG_itfBVGLinkFailure

Alarm	Attributes	Applicable major release
Name: ItfBVG_itfBVGLinkFailure (6017) Type: communicationsAlarm Package: femto.ItfBVG_itfBVGLinkFailure Raised on class: femto.ItfBVG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: This fault is raised when ItfBVG link failure is detected when no response id is received for keepalive messages on the BSR - BVG interface. This alarm is also sent when the initialising BVG binding update is not successful.		
Remedial action: Operator could check configuration of BVG IP address. If the problem persists, contact Nokia customer suppor		

Table 23-243 IuCSPrime_csCnConnectivityLost

Alarm	Attributes	Applicable major release
Name: IuCSPrime_csCnConnectivityLost (6023) Type: communicationsAlarm Package: femto.IuCSPrime_csCnConnectivityLost Raised on class: femto.IuCSPrime	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteNodeTransmissionError	Release: • 14.2
Description: The BSR has detected a loss of connectivity to the CS Core Network, even though the transport layer is still connected.		
Remedial action: The alarm is cleared by the Small Cell when connectivity to the CS Core Network is re-established. If the problem persists, contact Nokia customer support.		

Table 23-244 IuPSUplane_gTPEchoFailure

Alarm	Attributes	Applicable major release
Name: IuPSUplane_gTPEchoFailure (6043) Type: communicationsAlarm Package: femto.IuPSUplane_gTPEchoFailure Raised on class: femto.IuPSUplane	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: Echo failure on the IuPS interface.		
Remedial action: No operator intervention is required. If the problem persists, contact Nokia customer support.		

Table 23-245 jdbcactivecurrentconnectionscount

Alarm	Attributes	Applicable major release
Name: jdbcactivecurrentconnectionscount (6344) Type: equipmentAlarm Package: femto.jdbcactivecurrentconnectionscount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of connections currently in use by applications		

Table 23-245 jdbcactivecurrentconnectionscount (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-246 jdbcactivehighconnectionscount

Alarm	Attributes	Applicable major release
Name: jdbcactivehighconnectionscount (6345) Type: equipmentAlarm Package: femto.jdbcactivehighconnectionscount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Highest number of active database connections in this instance of the data source since the data source was instantiated		
Remedial action: Not available		

Table 23-247 jdbccurrcapacity

Alarm	Attributes	Applicable major release
Name: jdbccurrcapacity (6346) Type: equipmentAlarm Package: femto.jdbccurrcapacity Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Current database capacity		
Remedial action: Not available		

Table 23-248 jdbcdbsize

Alarm	Attributes	Applicable major release
Name: jdbcdbsize (6347) Type: equipmentAlarm Package: femto.jdbcdbsize Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: hdm database storage in use		
Remedial action: Not available		

Table 23-249 jdbcdevicecount

Alarm	Attributes	Applicable major release
Name: jdbcdevicecount (6348) Type: equipmentAlarm Package: femto.jdbcdevicecount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of devices defined in Home Device Manager		
Remedial action: Not available		

Table 23-250 jdbcenabledetpolicycount

Alarm	Attributes	Applicable major release
Name: jdbcenabledetpolicycount (6349) Type: equipmentAlarm Package: femto.jdbcenabledetpolicycount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of enabled and pending event-triggered policies defined in Home Device Manager		
Remedial action: Not available		

Table 23-251 jdbcenableditpolicycount

Alarm	Attributes	Applicable major release
Name: jdbcenableditpolicycount (6350) Type: equipmentAlarm Package: femto.jdbcenableditpolicycount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of enabled instant-triggered policies defined in Home Device Manager		
Remedial action: Not available		

Table 23-252 jdbcfailedactications

Alarm	Attributes	Applicable major release
Name: jdbcfailedactications (6351) Type: equipmentAlarm Package: femto.jdbcfailedactications Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of devices stated as activation failed in Home Device Manager		
Remedial action: Not available		

Table 23-253 jdbcfailedloginrate

Alarm	Attributes	Applicable major release
Name: jdbcfailedloginrate (6352) Type: equipmentAlarm Package: femto.jdbcfailedloginrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of failed attempts of devices to Home Device Manager		
Remedial action: Not available		

Table 23-254 jdbcfailedreserverequestcount

Alarm	Attributes	Applicable major release
Name: jdbcfailedreserverequestcount (6353) Type: equipmentAlarm Package: femto.jdbcfailedreserverequestcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The Number of reserve request failed.		
Remedial action: Not available		

Table 23-255 jdbcleakedconnectioncount

Alarm	Attributes	Applicable major release
Name: jdbcleakedconnectioncount (6354) Type: equipmentAlarm Package: femto.jdbcleakedconnectioncount Raised on class: femto.HDMCluster	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of leaked database connection		
Remedial action: Not available		

Table 23-256 jdbcmanagementpolicycount

Alarm	Attributes	Applicable major release
Name: jdbcmanagementpolicycount (6355) Type: equipmentAlarm Package: femto.jdbcmanagementpolicycount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of management policies defined in Home Device Manager		
Remedial action: Not available		

Table 23-257 jdbcpendingactivations

Alarm	Attributes	Applicable major release
Name: jdbcpendingactivations (6356) Type: equipmentAlarm Package: femto.jdbcpendingactivations Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Number of devices stated as activation pending in Home Device Manager		
Remedial action: Not available		

Table 23-258 jdbcwaitingcurrentconnectionscount

Alarm	Attributes	Applicable major release
Name: jdbcwaitingcurrentconnectionscount (6357) Type: equipmentAlarm Package: femto.jdbcwaitingcurrentconnectionscount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of connection requests waiting for a database connection		
Remedial action: Not available		

Table 23-259 jmsconnectionrequestcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsconnectionrequestcurrentcount (6358) Type: equipmentAlarm Package: femto.jmsconnectionrequestcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on connectionRequestQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-260 jmsconnectionrequestpendingcount

Alarm	Attributes	Applicable major release
Name: jmsconnectionrequestpendingcount (6359) Type: equipmentAlarm Package: femto.jmsconnectionrequestpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on connectionRequestQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-261 jmsconnectionrequestrate

Alarm	Attributes	Applicable major release
Name: jmsconnectionrequestrate (6360) Type: equipmentAlarm Package: femto.jmsconnectionrequestrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received Connection Request rate stored on connectionRequestQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-262 jmsdarcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsdarcurrentcount (6361) Type: equipmentAlarm Package: femto.jmsdarcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on deviceActionResultQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-263 jmsdarpendingcount

Alarm	Attributes	Applicable major release
Name: jmsdarpendingcount (6362) Type: equipmentAlarm Package: femto.jmsdarpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on deviceActionResultQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-264 jmsdarrate

Alarm	Attributes	Applicable major release
Name: jmsdarrate (6363) Type: equipmentAlarm Package: femto.jmsdarrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Received device action result rate		

Table 23-264 jmsdarrate (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-265 jmseventsrate

Alarm	Attributes	Applicable major release
Name: jmseventsrate (6364) Type: equipmentAlarm Package: femto.jmseventsrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Received inform event rate		
Remedial action: Not available		

Table 23-266 jmsinformeventscurrentcount

Alarm	Attributes	Applicable major release
Name: jmsinformeventscurrentcount (6365) Type: equipmentAlarm Package: femto.jmsinformeventscurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on deviceEventQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-267 jmsinformeventspendingcount

Alarm	Attributes	Applicable major release
Name: jmsinformeventspendingcount (6366) Type: equipmentAlarm Package: femto.jmsinformeventspendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on deviceEventQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-268 jmsnbiinternalcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsnbiinternalcurrentcount (6367) Type: equipmentAlarm Package: femto.jmsnbiinternalcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on nbiInternalQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-269 jmsnbiinternalpendingcount

Alarm	Attributes	Applicable major release
Name: jmsnbiinternalpendingcount (6368) Type: equipmentAlarm Package: femto.jmsnbiinternalpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on nbiInternalQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-270 jmsnbiinternalrate

Alarm	Attributes	Applicable major release
Name: jmsnbiinternalrate (6369) Type: equipmentAlarm Package: femto.jmsnbiinternalrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received NBI Out Bound Event rate stored on nbiInternalQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-271 jmsnbiobalarmcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobalarmcurrentcount (6370) Type: equipmentAlarm Package: femto.jmsnbiobalarmcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on nbiOutBoundAlarmTopic JMS destination for the current server		

Table 23-271 jmsnbiobalarmcurrentcount (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not available		

Table 23-272 jmsnbiobalarmpendingcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobalarmpendingcount (6371) Type: equipmentAlarm Package: femto.jmsnbiobalarmpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on nbiOutBoundAlarmTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-273 jmsnbiobalarmrate

Alarm	Attributes	Applicable major release
Name: jmsnbiobalarmrate (6372) Type: equipmentAlarm Package: femto.jmsnbiobalarmrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received NBI Out Bound Alarm rate stored on nbiOutBoundAlarmTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-274 jmsnbiobcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobcurrentcount (6373) Type: equipmentAlarm Package: femto.jmsnbiobcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on nbiOutBoundQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-275 jmsnbiobeventcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobeventcurrentcount (6374) Type: equipmentAlarm Package: femto.jmsnbiobeventcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on nbiOutBoundEventTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-276 jmsnbiobeventpendingcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobeventpendingcount (6375) Type: equipmentAlarm Package: femto.jmsnbiobeventpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on nbiOutBoundEventTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-277 jmsnbiobeventrate

Alarm	Attributes	Applicable major release
Name: jmsnbiobeventrate (6376) Type: equipmentAlarm Package: femto.jmsnbiobeventrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received NBI Out Bound Event rate stored on nbiOutBoundEventTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-278 jmsnbiobpendingcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobpendingcount (6377) Type: equipmentAlarm Package: femto.jmsnbiobpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2

Table 23-278 jmsnbiobpendingcount (continued)

Alarm	Attributes	Applicable major release
Description: The current number of messages pending (unacknowledged or uncommitted) stored on nbiOutBoundQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-279 jmsnbiobrate

Alarm	Attributes	Applicable major release
Name: jmsnbiobrate (6378) Type: equipmentAlarm Package: femto.jmsnbiobrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received NBI Out Bound Event rate stored on nbiOutBoundQueue JMS destination for the current server		
Remedial action: Not available		

Table 23-280 jmsnbiobresultcurrentcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobresultcurrentcount (6379) Type: equipmentAlarm Package: femto.jmsnbiobresultcurrentcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages stored on nbiOutBoundResultTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-281 jmsnbiobresultpendingcount

Alarm	Attributes	Applicable major release
Name: jmsnbiobresultpendingcount (6380) Type: equipmentAlarm Package: femto.jmsnbiobresultpendingcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of messages pending (unacknowledged or uncommitted) stored on nbiOutBoundResultTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-282 jmsnbiobresultrate

Alarm	Attributes	Applicable major release
Name: jmsnbiobresultrate (6381) Type: equipmentAlarm Package: femto.jmsnbiobresultrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The current number of received NBI Out Bound Result rate stored on nbiOutBoundResultTopic JMS destination for the current server		
Remedial action: Not available		

Table 23-283 jtaactivetxcount

Alarm	Attributes	Applicable major release
Name: jtaactivetxcount (6382) Type: equipmentAlarm Package: femto.jtaactivetxcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The total number of active transacions on the server		
Remedial action: Not available		

Table 23-284 jtacommittedtxrate

Alarm	Attributes	Applicable major release
Name: jtacommittedtxrate (6383) Type: equipmentAlarm Package: femto.jtacommittedtxrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Total number of transactions committed by this server		
Remedial action: Not available		

Table 23-285 jtarolledbacktxrate

Alarm	Attributes	Applicable major release
Name: jtarolledbacktxrate (6384) Type: equipmentAlarm Package: femto.jtarolledbacktxrate Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Total number of transactions rolled back by this server		
Remedial action: Not available		

Table 23-286 jvmfreeheapsize

Alarm	Attributes	Applicable major release
Name: jvmfreeheapsize (6385) Type: equipmentAlarm Package: femto.jvmfreeheapsize Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of free heap size availabe in JVM		
Remedial action: Not available		

Table 23-287 jvmheapfreepercent

Alarm	Attributes	Applicable major release
Name: jvmheapfreepercent (6386) Type: equipmentAlarm Package: femto.jvmheapfreepercent Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The percentage of free heap available in JVM		
Remedial action: Not available		

Table 23-288 jvmheapsize

Alarm	Attributes	Applicable major release
Name: jvmheapsize (6387) Type: equipmentAlarm Package: femto.jvmheapsize Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The heap size of JVM		
Remedial action: Not available		

Table 23-289 jvmmaxheapsize

Alarm	Attributes	Applicable major release
Name: jvmmaxheapsize (6388) Type: equipmentAlarm Package: femto.jvmmaxheapsize Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The maximum heap size of JVM		
Remedial action: Not available		

Table 23-290 LBO_lboServiceUnavailable

Alarm	Attributes	Applicable major release
Name: LBO_lboServiceUnavailable (12994) Type: processingErrorAlarm Package: femto.LBO_lboServiceUnavailable Raised on class: femto.LBO	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: This fault is created when one or more LBO subsystems have some unrecoverable error or failed.		
Remedial action: Operator needs to initiate the FAP reboot to clear the alarm.		

Table 23-291 LBO_lgwIpPoolExhausted

Alarm	Attributes	Applicable major release
Name: LBO_lgwIpPoolExhausted (12995) Type: processingErrorAlarm Package: femto.LBO_lgwIpPoolExhausted Raised on class: femto.LBO	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2
Description: LGW has exhausted IP addresses and no new UEs can use LBO service.		
Remedial action: No operator action required. The alarm will be cleared as soon as some of the existing UEs are detached resulting in release of allocated IP addresses		

Table 23-292 LBO_lgwS5GtpEchoFailure

Alarm	Attributes	Applicable major release
Name: LBO_lgwS5GtpEchoFailure (12996) Type: qualityOfServiceAlarm Package: femto.LBO_lgwS5GtpEchoFailure Raised on class: femto.LBO	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: Echo failure on all the S5 interfaces.		
Remedial action: Operator intervention is not required. The alarm will be cleared by the Femtocell following a successful S5 GTP Echo response atleast from one SGW.		

Table 23-293 LBO_lgwS5SgwExceeded

Alarm	Attributes	Applicable major release
Name: LBO_lgwS5SgwExceeded (12997) Type: processingErrorAlarm Package: femto.LBO_lgwS5SgwExceeded Raised on class: femto.LBO	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2

Table 23-293 LBO_lgwS5SgwExceeded (continued)

Alarm	Attributes	Applicable major release
Description: LGW could not allocate new SGW Context as max number of SGWs exceeded		
Remedial action: The alarm will be cleared as-soon-as all UEs belonging to an existing SGW are deallocated resulting in SGW context deletion		

Table 23-294 LCell_candidateNeighbourIdentified

Alarm	Attributes	Applicable major release
Name: LCell_candidateNeighbourIdentified (6059) Type: processingErrorAlarm Package: femto.LCell_candidateNeighbourIdentified Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: In static mode neighbour list optimisation, on evaluation that a cell should be added to the neighbour list as per dynamic mode checks, the Small Cell AP shall raise an alarm, containing relevant additional information. This alarm shall be cleared by a reboot or manual addition of the candidate as a neighbour.		
Remedial action: Operator to verify if the cell reported in the alarm should be added manually to neighbor list. If it is added manually, this alarm gets cleared. Else, this alarm is cleared on next reboot. This is also an indication to operator if nloEnableDynamicNLO has to be changed to true from false. nloEnableDynamicNLO when set to false is static mode neighbor list optimisation, else it is dynamic mod		

Table 23-295 LCell_carrierReSelectionNotPossible

Alarm	Attributes	Applicable major release
Name: LCell_carrierReSelectionNotPossible (6060) Type: operationalViolation Package: femto.LCell_carrierReSelectionNotPossible Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The fault is raised when no carrier for the FBSR could be selected under different situations, which are detailed in AdditionalText.		
Remedial action: No operator intervention is required		

Table 23-296 LCell_centralisedAssignmentFailed

Alarm	Attributes	Applicable major release
Name: LCell_centralisedAssignmentFailed (8494) Type: processingErrorAlarm Package: femto.LCell_centralisedAssignmentFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2

Table 23-296 LCell_centralisedAssignmentFailed (continued)

Alarm	Attributes	Applicable major release
Description: The SCGW associated with this Access Point has refused to assign a PSC to this access point		
Remedial action: Check the Access Point and Gateway PSC's femto group configuration to make sure they are consistent.		

Table 23-297 LCell_centralisedAssignmentFailedNoPSC

Alarm	Attributes	Applicable major release
Name: LCell_centralisedAssignmentFailedNoPSC (8495) Type: processingErrorAlarm Package: femto.LCell_ centralisedAssignmentFailedNoPSC Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The SCGW associated with this Access Point has refused to assign a PSC to this access point, however, the Access Point does not have a valid PSC assigned		
Remedial action: Check the Access Point's configuration to see why no PSC was assigned. If necessary, assign a valid PSC manually.		

Table 23-298 LCell_channelConfigBCHFailed

Alarm	Attributes	Applicable major release
Name: LCell_channelConfigBCHFailed (6061) Type: operationalViolation Package: femto.LCell_channelConfigBCHFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The configuration of the Common Channel BCH failed.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-299 LCell_channelConfigFACHFailed

Alarm	Attributes	Applicable major release
Name: LCell_channelConfigFACHFailed (6062) Type: operationalViolation Package: femto.LCell_channelConfigFACHFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The configuration of the Common Transport Channel for FACH failed.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-300 LCell_channelConfigPCHFailed

Alarm	Attributes	Applicable major release
Name: LCell_channelConfigPCHFailed (6063) Type: operationalViolation Package: femto.LCell_channelConfigPCHFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The configuration of the Common Transport Channel for PCH failed.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-301 LCell_channelConfigPRACHFailed

Alarm	Attributes	Applicable major release
Name: LCell_channelConfigPRACHFailed (6064) Type: operationalViolation Package: femto.LCell_channelConfigPRACHFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The configuration of the Common Transport Channel for PRACH failed.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-302 LCell_codeAllocationFailure

Alarm	Attributes	Applicable major release
Name: LCell_codeAllocationFailure (6065) Type: processingErrorAlarm Package: femto.LCell_codeAllocationFailure Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: Channelisation code allocation failure.		
Remedial action: The alarm will be cleared by the Small Cell following reset. If the problem persists, contact Nokia customer support.		

Table 23-303 LCell_commonMeasInitTimeout

Alarm	Attributes	Applicable major release
Name: LCell_commonMeasInitTimeout (6066) Type: processingErrorAlarm Package: femto.LCell_commonMeasInitTimeout Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: No response from BRRC on the initiation of a common measurement.		

Table 23-303 LCell_commonMeasInitTimeout (continued)

Alarm	Attributes	Applicable major release
Remedial action: No operator intervention is required. If the problem persists, contact Nokia customer support		

Table 23-304 LCell_cpBlockRequestTimeout

Alarm	Attributes	Applicable major release
Name: LCell_cpBlockRequestTimeout (6067) Type: processingErrorAlarm Package: femto.LCell_cpBlockRequestTimeout Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: No response from BRRM to a Block Resource Request received from BRRC.		
Remedial action: The alarm will be cleared by the Small Cell following reset. If the problem persists, contact Nokia customer support.		

Table 23-305 LCell_dLCongestion

Alarm	Attributes	Applicable major release
Name: LCell_dLCongestion (6068) Type: qualityOfServiceAlarm Package: femto.LCell_dLCongestion Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 14.2
Description: This fault is raised when the condition for DL congestion is met. The BSR starts the DL congestion control algorithm to clear the congestion.		
Remedial action: The alarm will be cleared by the Small Cell once the DL congestion has been cleared by the DL congestion control algorithm. If the problem persists, contact Nokia customer support.		

Table 23-306 LCell_dpdTraining

Alarm	Attributes	Applicable major release
Name: LCell_dpdTraining (8496) Type: processingErrorAlarm Package: femto.LCell_dpdTraining Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitterFailure	Release: • 14.2
Description: DPD training failure. SW detects either of the two following conditions for five training requests in a row; The DPD training request returns a failure status or the measured ACLR does not meet the thresholds defined in the hardware config file.		
Remedial action: MS MCI logs the fault. This fault may be caued by hardware failure. If the problem persists, contact Nokia customer support		

Table 23-307 LCell_hsbitratemeasInitFail

Alarm	Attributes	Applicable major release
Name: LCell_hsbitratemeasInitFail (6070) Type: operationalViolation Package: femto.LCell_hsbitratemeasInitFail Raised on class: femto.LCell	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the HS-DSCH provided bit rate measurement failed.		
Remedial action: This alarm does not require operator intervention.		

Table 23-308 LCell_hsbitratemeasStop

Alarm	Attributes	Applicable major release
Name: LCell_hsbitratemeasStop (6071) Type: operationalViolation Package: femto.LCell_hsbitratemeasStop Raised on class: femto.LCell	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The HS-DSCH provided bit rate measurement discontinued.		
Remedial action: This alarm does not require operator intervention.		

Table 23-309 LCell_hsTxCarrierPowermeasInitFail

Alarm	Attributes	Applicable major release
Name: LCell_hsTxCarrierPowermeasInitFail (6069) Type: operationalViolation Package: femto.LCell_hsTxCarrierPowermeasInitFail Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the common measurements of the transmitted carrier power of all codes not used for HS-PDSCH or HS-SCCH transmission failed.		
Remedial action: This alarm does not require operator intervention		

Table 23-310 LCell_inconsistentDetectedCellInfo

Alarm	Attributes	Applicable major release
Name: LCell_inconsistentDetectedCellInfo (6072) Type: processingErrorAlarm Package: femto.LCell_inconsistentDetectedCellInfo Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2

Table 23-310 LCell_inconsistentDetectedCellInfo (continued)

Alarm	Attributes	Applicable major release
Description: The Small Cell AP shall raise an alarm if it detects via network listening that a manually configured neighbour has incorrect configuration data. This alarm shall be cleared on reboot and/or any change to manually configured neighbours.Note: This was previously only SysLogged in BCR4.3. It is triggered if there are inconsistencies between the femtos own data and the detected BSRid, FDD Freq band, uARFCN uplink and downlink or RNCid. It is also triggered if the sniffed data is incomplete.		
Remedial action: Operator to verify the reported inconsistency in uARFCNDl/Ul and / or Frequency Band and / or RNCId, and if required, manually change the inconsistency. When inconsistency is corrected manually, this alarm is cleared, else this alarm gets cleared on next reboot.		

Table 23-311 LCell_invalidSIBParameter

Alarm	Attributes	Applicable major release
Name: LCell_invalidSIBParameter (6073) Type: processingErrorAlarm Package: femto.LCell_invalidSIBParameter Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: CSIB has detected an invalid SIB parameter, and no update of SIBs is performed towards CCC.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-312 LCell_invalidSIBSchedule

Alarm	Attributes	Applicable major release
Name: LCell_invalidSIBSchedule (6074) Type: processingErrorAlarm Package: femto.LCell_invalidSIBSchedule Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: CSIB has detected an invalid SIB schedule, and no update of SIBs is performed towards CCC.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-313 LCell_neighbourListUpdate

Alarm	Attributes	Applicable major release
Name: LCell_neighbourListUpdate (6075) Type: processingErrorAlarm Package: femto.LCell_neighbourListUpdate Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2

Table 23-313 LCell_neighbourListUpdate (continued)

Alarm	Attributes	Applicable major release
Description: On evaluation of a new neighbour list, the Small Cell AP shall send an informational, non-critical alarm to the OAM system detailing the old and the new lists.Note: Alarm payload is limited to 250 characters, so the alarm with detail the complete new list, with a sequence of adds and subtractions detailing the change from the previous list. The Small Cell AP shall raise one alarm for intra-frequency neighbours, and one for inter-frequency neighbours		
Remedial action: No operator action is required. Just an informational alarm, giving list of cells newly added and / or removed from neighbor lists. This alarm gets cleared after reboot		

Table 23-314 LCell_neighbourNotMeetingQualityCriteria

Alarm	Attributes	Applicable major release
Name: LCell_neighbourNotMeetingQualityCriteria (6076) Type: processingErrorAlarm Package: femto.LCell_ neighbourNotMeetingQualityCriteria Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: On a neighbour cell failing quality checks, either at the end of a monitoring period or on the daily check, the Small Cell AP shall raise an alarm, detailing the failing cell ID and performance metric. This alarm shall be cleared automatically if the neighbour is removed by the operator or a subsequent operation of this algorithm in 'dynamic' mode.		
Remedial action: No operator intervention required, but alarm will be cleared automatically when it gets re-evaluated next day. If issue persists, a new alarm will be raised. This alarm is an informational alarm.Or this alarm gets cleared at the next reboot. This alarm is applicable for all type of cells, viz., Configured, Detected, Informed, UE Detected. Not applicable for UE Detected Pending		

Table 23-315 LCell_rACHmeasInitFail

Alarm	Attributes	Applicable major release
Name: LCell_rACHmeasInitFail (6077) Type: operationalViolation Package: femto.LCell_rACHmeasInitFail Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the RACH measurement failed.		
Remedial action: This alarm is cleared by the Small Cell once the measurement initialization succeeds. If the problem persists, contact Nokia customer support.		

Table 23-316 LCell_rACHmeasStop

Alarm	Attributes	Applicable major release
Name: LCell_rACHmeasStop (6078) Type: operationalViolation Package: femto.LCell_rACHmeasStop Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The RACH measurement discontinued.		
Remedial action: This alarm does not require operator intervention.		

Table 23-317 LCell_rfCalibrationFailure

Alarm	Attributes	Applicable major release
Name: LCell_rfCalibrationFailure (8180) Type: processingErrorAlarm Package: femto.LCell_rfCalibrationFailure Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The cell configuration is attempting to use an RF path that has not been calibrated.		
Remedial action: The cell configuration parameters must be modified to align with the RF capabilities. If the cell configuration is correct then the MS MCI may need RF calibration.		

Table 23-318 LCell_rfConfigurationFailure

Alarm	Attributes	Applicable major release
Name: LCell_rfConfigurationFailure (8181) Type: processingErrorAlarm Package: femto.LCell_rfConfigurationFailure Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The cell configuration is not compatible with the MS MCI RF hardware.		
Remedial action: The cell configuration parameters must be modified to align with the RF capabilities. For example, the configured ARFCN/Band or transmit power settings must be within the supported range of the MS MCI.		

Table 23-319 LCell_rfRxDiversityFailure

Alarm	Attributes	Applicable major release
Name: LCell_rfRxDiversityFailure (8182) Type: equipmentAlarm Package: femto.LCell_rfRxDiversityFailure Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2

Table 23-319 LCell_rfRxDiversityFailure (continued)

Alarm	Attributes	Applicable major release
Description: Diversity reception is enabled and there is an imbalance between the receive signal levels.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure, damage to the integrated antenna or its RF connections, or (if used) any external antenna or antenna cable or connector. If the problem persists, contact Nokia customer support		

Table 23-320 LCell_rfRxFailure

Alarm	Attributes	Applicable major release
Name: LCell_rfRxFailure (8183) Type: equipmentAlarm Package: femto.LCell_rfRxFailure Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The RF receiver for this cell has failed.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure or possibly to a timing problem.		

Table 23-321 LCell_rfTemperatureCritical

Alarm	Attributes	Applicable major release
Name: LCell_rfTemperatureCritical (8184) Type: environmentalAlarm Package: femto.LCell_rfTemperatureCritical Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2
Description: RF components supporting this cell are outside operating temperature limits.		
Remedial action: The unit is currently too cold or too warm, move it to location within the specified operating temperature range.		

Table 23-322 LCell_rfTemperatureWarning

Alarm	Attributes	Applicable major release
Name: LCell_rfTemperatureWarning (8185) Type: environmentalAlarm Package: femto.LCell_rfTemperatureWarning Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2
Description: RF components supporting this cell are near operating temperature limits.		
Remedial action: The unit is currently too cold or too warm, move it to location within the specified operating temperature range.		

Table 23-323 LCell_rfTxFailure

Alarm	Attributes	Applicable major release
Name: LCell_rfTxFailure (8186) Type: equipmentAlarm Package: femto.LCell_rfTxFailure Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The RF transmitter for this cell has failed.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure or possibly to a timing problem. If the problem persists, contact Nokia customer support		

Table 23-324 LCell_rfTxPowerCritical

Alarm	Attributes	Applicable major release
Name: LCell_rfTxPowerCritical (8187) Type: equipmentAlarm Package: femto.LCell_rfTxPowerCritical Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitterFailure	Release: • 14.2
Description: RF transmit power for this cell exceeds hardware operating limits.		
Remedial action: The cell power is too high, configure a lower transmit power.		

Table 23-325 LCell_rfTxPowerWarning

Alarm	Attributes	Applicable major release
Name: LCell_rfTxPowerWarning (8188) Type: equipmentAlarm Package: femto.LCell_rfTxPowerWarning Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitterFailure	Release: • 14.2
Description: RF transmit power for this cell is higher than expected.		
Remedial action: The cell power is too high, configure a lower transmit power.		

Table 23-326 LCell_rSSImeasInitFail

Alarm	Attributes	Applicable major release
Name: LCell_rSSImeasInitFail (6079) Type: operationalViolation Package: femto.LCell_rSSImeasInitFail Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the RSSI measurement failed.		

Table 23-326 LCell_rSSImeasInitFail (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.		

Table 23-327 LCell_rSSImeasStop

Alarm	Attributes	Applicable major release
Name: LCell_rSSImeasStop (6080) Type: operationalViolation Package: femto.LCell_rSSImeasStop Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The RSSI measurement discontinued.		
Remedial action: This alarm does not require operator intervention.		

Table 23-328 LCell_sharedChannelConfigHSPAFailed

Alarm	Attributes	Applicable major release
Name: LCell_sharedChannelConfigHSPAFailed (6082) Type: operationalViolation Package: femto.LCell_ sharedChannelConfigHSPAFailed Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the Shared Channel for HSDPA/HSUPA failed.		
Remedial action: This alarm is cleared by the Small Cell after the Small Cell resets. If the problem persists, contact Nokia customer support.If the problem persists, contact Nokia customer support		

Table 23-329 LCell_sIBUpdateCCCError

Alarm	Attributes	Applicable major release
Name: LCell_sIBUpdateCCCError (6081) Type: operationalViolation Package: femto.LCell_sIBUpdateCCCError Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The SIB update was not performed within CCC, the CCC specific error cause is returned.		
Remedial action: No operator intervention is required. If the problem persists, contact Nokia customer support		

Table 23-330 LCell_sleepingCellDetected

Alarm	Attributes	Applicable major release
Name: LCell_sleepingCellDetected (11156) Type: processingErrorAlarm Package: femto.LCell_sleepingCellDetected Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: performanceDegraded	Release: • 14.2
Description: This alarm reports sleeping cell detected state, which is triggered when cell is not serving traffic or serving reduced traffic when it should be operational.		
Remedial action: In some case, MSAP automatically reset when the alarm is triggered. If this alarm persists, reset the MSAP.		

Table 23-331 LCell_spareLCellAlarm1

Alarm	Attributes	Applicable major release
Name: LCell_spareLCellAlarm1 (8189) Type: processingErrorAlarm Package: femto.LCell_spareLCellAlarm1 Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-332 LCell_spareLCellAlarm2

Alarm	Attributes	Applicable major release
Name: LCell_spareLCellAlarm2 (8190) Type: processingErrorAlarm Package: femto.LCell_spareLCellAlarm2 Raised on class: femto.LCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-333 LCell_spareLCellAlarm3

Alarm	Attributes	Applicable major release
Name: LCell_spareLCellAlarm3 (8191) Type: processingErrorAlarm Package: femto.LCell_spareLCellAlarm3 Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-334 LCell_tpapReleaseIndFACH

Alarm	Attributes	Applicable major release
Name: LCell_tpapReleaseIndFACH (6085) Type: operationalViolation Package: femto.LCell_tpapReleaseIndFACH Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Tpap release indication for FACH was received by BRRM.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support		

Table 23-335 LCell_tpapReleaseIndPCH

Alarm	Attributes	Applicable major release
Name: LCell_tpapReleaseIndPCH (6086) Type: operationalViolation Package: femto.LCell_tpapReleaseIndPCH Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Tpap release indication for PCH was received by BRRM.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support		

Table 23-336 LCell_tpapReleaseIndRACH

Alarm	Attributes	Applicable major release
Name: LCell_tpapReleaseIndRACH (6087) Type: operationalViolation Package: femto.LCell_tpapReleaseIndRACH Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Tpap release indication for RACH was received by BRRM.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support		

Table 23-337 LCell_tSSImeasInitFail

Alarm	Attributes	Applicable major release
Name: LCell_tSSImeasInitFail (6083) Type: operationalViolation Package: femto.LCell_tSSImeasInitFail Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The initiation of the TSSI measurement failed.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-338 LCell_tSSImeasStop

Alarm	Attributes	Applicable major release
Name: LCell_tSSImeasStop (6084) Type: operationalViolation Package: femto.LCell_tSSImeasStop Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: The TSSI measurement discontinued.		
Remedial action: This alarm does not require operator intervention.		

Table 23-339 LCell_uLCongestion

Alarm	Attributes	Applicable major release
Name: LCell_uLCongestion (6088) Type: qualityOfServiceAlarm Package: femto.LCell_uLCongestion Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 14.2
Description: This fault is raised when the condition for UL congestion is met. The BSR starts the UL congestion control algorithm to clear the congestion.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-340 LCell_unknownCandidateNeighboursPSC

Alarm	Attributes	Applicable major release
Name: LCell_unknownCandidateNeighboursPSC (6089) Type: processingErrorAlarm Package: femto.LCell_ unknownCandidateNeighboursPSC Raised on class: femto.LCell	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: If no candidate cells are identified, or if all candidates fail the quality checks after their monitoring periods, the Small Cell AP shall raise the alarm, containing the PSC and any candidate cell list as additional information.This alarm is cleared by reboot or the modification of manually configured neighbours for this Small Cell AP. The Small Cell AP shall maintain the received information until the alarm has been cleared to prevent raising the same alarm multiple times for the same PSC.		
Remedial action: Operator can manually add the UE reported candidate cells, that failed HO quality check criteria, to neighbor lists. If they are added manually, this alarm gets cleared. Else, this alarm is cleared on next reboot.		

Table 23-341 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 14.2
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 23-342 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 14.2
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 23-343 LteCell_collidingPciSelected

Alarm	Attributes	Applicable major release
Name: LteCell_collidingPciSelected (11157) Type: processingErrorAlarm Package: femto.LteCell_collidingPciSelected Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is raised to indicate that SON was unable to select a clean PCI and is now operating in a PCI that is in collision		
Remedial action: NA		

Table 23-344 LteCell_lteOamCellOperationFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteOamCellOperationFailure (12405) Type: processingErrorAlarm Package: femto.LteCell_lteOamCellOperationFailure Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: This alarm is generated, when internal cell related autonomous operations (such as cell config/delete/start/stop, RF enable/disable, acquiring resource from FTRM) fails. These autonomous operations are caused by events such S1 link loss, PCI reselection, OSDL starting unlicensed cell etc. This alarm is raised on certain internal fault conditions. This alarm is added for timely recovery of the FAP, if it ever gets into this condition.		
Remedial action: No action needed from the operator. AP is rebooted by Nokia OAM		

Table 23-345 LteCell_lteOamConfigurationFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteOamConfigurationFailure (6092) Type: processingErrorAlarm Package: femto.LteCell_lteOamConfigurationFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: LTE OAM configuration failure alarm		
Remedial action: NA		

Table 23-346 LteCell_lteRfCalibrationFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfCalibrationFailure (8192) Type: processingErrorAlarm Package: femto.LteCell_lteRfCalibrationFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The cell configuration is attempting to use an RF path that has not been calibrated.		
Remedial action: The cell configuration parameters must be modified to align with the RF capabilities. If the cell configuration is correct then the MS MCI may need RF calibration.		

Table 23-347 LteCell_lteRfConfigurationFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfConfigurationFailure (8193) Type: processingErrorAlarm Package: femto.LteCell_lteRfConfigurationFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The cell configuration is not compatible with the MS MCI RF hardware.		
Remedial action: The cell configuration parameters must be modified to align with the RF capabilities. For example, the configured ARFCN/Band or transmit power settings must be within the supported range of the MS MCI.		

Table 23-348 LteCell_lteRfRxDiversityFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfRxDiversityFailure (8194) Type: equipmentAlarm Package: femto.LteCell_lteRfRxDiversityFailure Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Diversity reception is enabled and there is an imbalance between the receive signal levels.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure, damage to the integrated antenna or its RF connections, or (if used) any external antenna or antenna cable or connector.		

Table 23-349 LteCell_lteRfRxFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfRxFailure (8195) Type: equipmentAlarm Package: femto.LteCell_lteRfRxFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The RF receiver for this cell has failed.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure or possibly to a timing problem.		

Table 23-350 LteCell_lteRfTemperatureCritical

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfTemperatureCritical (8196) Type: environmentalAlarm Package: femto.LteCell_lteRfTemperatureCritical Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2

Table 23-350 LteCell_lteRfTemperatureCritical (continued)

Alarm	Attributes	Applicable major release
Description: RF components supporting this cell are outside operating temperature limits.		
Remedial action: The unit is currently too cold or too warm, move it to location within the specified operating temperature range.		

Table 23-351 LteCell_lteRfTemperatureWarning

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfTemperatureWarning (8197) Type: environmentalAlarm Package: femto.LteCell_lteRfTemperatureWarning Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2
Description: RF components supporting this cell are near operating temperature limits.		
Remedial action: The unit is currently too cold or too warm, move it to location within the specified operating temperature range.#		

Table 23-352 LteCell_lteRfTxFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfTxFailure (8198) Type: equipmentAlarm Package: femto.LteCell_lteRfTxFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The RF transmitter for this cell has failed.		
Remedial action: MS MCI logs the fault. The fault may be due to an RF hardware failure or possibly to a timing problem.		

Table 23-353 LteCell_lteRfTxPowerCritical

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfTxPowerCritical (8199) Type: equipmentAlarm Package: femto.LteCell_lteRfTxPowerCritical Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitterFailure	Release: • 14.2
Description: RF transmit power for this cell exceeds hardware operating limits.		
Remedial action: The cell power is too high, configure a lower transmit power.		

Table 23-354 LteCell_lteRfTxPowerWarning

Alarm	Attributes	Applicable major release
Name: LteCell_lteRfTxPowerWarning (8200) Type: equipmentAlarm Package: femto.LteCell_lteRfTxPowerWarning Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitterFailure	Release: • 14.2
Description: RF transmit power for this cell is higher than expected.		
Remedial action: The cell power is too high, configure a lower transmit power.		

Table 23-355 LteCell_lteRrcSctpAssociationFailure

Alarm	Attributes	Applicable major release
Name: LteCell_lteRrcSctpAssociationFailure (6093) Type: communicationsAlarm Package: femto.LteCell_lteRrcSctpAssociationFailure Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError	Release: • 14.2
Description: RRC/SCTP association failure alarm. This alarm is triggered by: 1) eNB receives an ErrorInd from MME with Criticality Diagnostics; 2) S1Setup response timer expires and maximum retries exhausted; 3) receive S1Setup Failure from MME and maximum retries exhausted; 4) during S1Setup, SCTP conn failure; 5) SCTP s1 setup req send fails; 6) upon expiration of sctp connection recovery timer; 7) gets sctp shutdown from mme when cell is up.		
Remedial action: NA		

Table 23-356 LteCell_lteSleepingCellDetected

Alarm	Attributes	Applicable major release
Name: LteCell_lteSleepingCellDetected (11158) Type: processingErrorAlarm Package: femto.LteCell_lteSleepingCellDetected Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: performanceDegraded	Release: • 14.2
Description: This alarm reports sleeping cell detected, which is triggered when cell is not serving traffic or serving reduced traffic when it should be operational.		
Remedial action: In some case, MSAP automatically reset when the alarm is triggered. If this alarm persists, reset the MSAP.		

Table 23-357 LteCell_pciCollisionResolutionInProgress

Alarm	Attributes	Applicable major release
Name: LteCell_pciCollisionResolutionInProgress (8201) Type: processingErrorAlarm Package: femto.LteCell_ pciCollisionResolutionInProgress Raised on class: femto.LteCell	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: A PCI collision between the cell and a neighbor one has been detected and a resolution attempt is in progress.		
Remedial action: No operator intervention is needed. A separate alarm will be generated if the resolution attempt fails.		

Table 23-358 LteCell_pciConfusionDetected

Alarm	Attributes	Applicable major release
Name: LteCell_pciConfusionDetected (12406) Type: processingErrorAlarm Package: femto.LteCell_pciConfusionDetected Raised on class: femto.LteCell	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This alarm is raised when AP identifies that two serving cell neighbors share the same PCI.The alarm shall be cleared when the MS-AP reboots.		
Remedial action: No action needed from the operator. The two serving cells which have the same PCI are informed and hence, they can choose different PCI		

Table 23-359 LteCell_pciSelectionFailure

Alarm	Attributes	Applicable major release
Name: LteCell_pciSelectionFailure (6094) Type: processingErrorAlarm Package: femto.LteCell_pciSelectionFailure Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: PCI selection failure alarm. SON detects no free PCI to be used from the provisioned list. Detected unused PCI. No RSI found for selected PCI.		
Remedial action: Reprovision PCI list		

Table 23-360 LteCell_spareLteCellAlarm1

Alarm	Attributes	Applicable major release
Name: LteCell_spareLteCellAlarm1 (8202) Type: processingErrorAlarm Package: femto.LteCell_spareLteCellAlarm1 Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details		

Table 23-361 LteCell_spareLteCellAlarm2

Alarm	Attributes	Applicable major release
Name: LteCell_spareLteCellAlarm2 (8203) Type: processingErrorAlarm Package: femto.LteCell_spareLteCellAlarm2 Raised on class: femto.LteCell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details		

Table 23-362 LteCell_spareLteCellAlarm3

Alarm	Attributes	Applicable major release
Name: LteCell_spareLteCellAlarm3 (8204) Type: processingErrorAlarm Package: femto.LteCell_spareLteCellAlarm3 Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details		

Table 23-363 LteCell_ueAuditContextMismatch

Alarm	Attributes	Applicable major release
Name: LteCell_ueAuditContextMismatch (11159) Type: processingErrorAlarm Package: femto.LteCell_ueAuditContextMismatch Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This alarm is raised when detects mismatched UE context between RRM-RRC or RRC internal modules UECC-LLIM, UECC-S1AP, UECC-X2AP, LLIM-S1U for mismatch threshold audit attempts. (This alarm is reserved for future use.)		
Remedial action: Reboot MSAP		

Table 23-364 LteCell_ueAuditGbrUsageMismatch

Alarm	Attributes	Applicable major release
Name: LteCell_ueAuditGbrUsageMismatch (11160) Type: processingErrorAlarm Package: femto.LteCell_ueAuditGbrUsageMismatch Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This alarm is raised when GBR usage limit threshold is reached and there are no active UEs currently in the system but used_dl_bitrate/used_ul_bitrate still has some value. (This alarm is reserved for future use.)		
Remedial action: Reboot MSAP		

Table 23-365 MetroDock_metroDockHWFailure

Alarm	Attributes	Applicable major release
Name: MetroDock_metroDockHWFailure (6101) Type: equipmentAlarm Package: femto.MetroDock_metroDockHWFailure Raised on class: femto.MetroDock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: This fault is raised when HW failure was detected in MetroDock or SFPs.		
Remedial action: Replace the metro dock connection box		

Table 23-366 MetroDock_metroDockReceivePathFailure

Alarm	Attributes	Applicable major release
Name: MetroDock_metroDockReceivePathFailure (6102) Type: communicationsAlarm Package: femto.MetroDock_ metroDockReceivePathFailure Raised on class: femto.MetroDock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised in case of fault in receive path.		
Remedial action: Replace the metro dock connection box		

Table 23-367 MetroDock_wifiNoSignalDetected

Alarm	Attributes	Applicable major release
Name: MetroDock_wifiNoSignalDetected (6103) Type: communicationsAlarm Package: femto.MetroDock_wifiNoSignalDetected Raised on class: femto.MetroDock	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2

Table 23-367 MetroDock_wifiNoSignalDetected (continued)

Alarm	Attributes	Applicable major release
Description: This fault is raised if signal of link status is not detected on the Wi-Fi Ethernet port.		
Remedial action: NA		

Table 23-368 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 14.2
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 23-369 multicastclustermessageslostcount

Alarm	Attributes	Applicable major release
Name: multicastclustermessageslostcount (6390) Type: equipmentAlarm Package: femto.multicastclustermessageslostcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Cluster Multicast lost message rate		
Remedial action: Not available		

Table 23-370 multicastcompletedrequests

Alarm	Attributes	Applicable major release
Name: multicastcompletedrequests (6391) Type: equipmentAlarm Package: femto.multicastcompletedrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Multicast completed request count		
Remedial action: Not available		

Table 23-371 multicastpendingrequests

Alarm	Attributes	Applicable major release
Name: multicastpendingrequests (6392) Type: equipmentAlarm Package: femto.multicastpendingrequests Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Multicast pending request count		
Remedial action: Not available		

Table 23-372 multipleBSRlinkloss

Alarm	Attributes	Applicable major release
Name: multipleBSRlinkloss (8212) Type: communicationsAlarm Package: femto.multipleBSRlinkloss Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: Multiple BSR are not reachable from HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes.		

Table 23-373 nbicapturedevice

Alarm	Attributes	Applicable major release
Name: nbicapturedevice (6393) Type: equipmentAlarm Package: femto.nbicapturedevice Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi captureDevice		
Remedial action: Not available		

Table 23-374 nbicapturedeviceavg

Alarm	Attributes	Applicable major release
Name: nbicapturedeviceavg (6394) Type: equipmentAlarm Package: femto.nbicapturedeviceavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi captureDevice.avg		
Remedial action: Not available		

Table 23-375 nbiclearalarm

Alarm	Attributes	Applicable major release
Name: nbiclearalarm (6395) Type: equipmentAlarm Package: femto.nbiclearalarm Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi clearAlarm		
Remedial action: Not available		

Table 23-376 nbiclearalarmavg

Alarm	Attributes	Applicable major release
Name: nbiclearalarmavg (6396) Type: equipmentAlarm Package: femto.nbiclearalarmavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi clearAlarm.avg		
Remedial action: Not available		

Table 23-377 nbicreatedevice

Alarm	Attributes	Applicable major release
Name: nbicreatedevice (6397) Type: equipmentAlarm Package: femto.nbicreatedevice Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi createDevice		
Remedial action: Not available		

Table 23-378 nbicreatedeviceavg

Alarm	Attributes	Applicable major release
Name: nbicreatedeviceavg (6398) Type: equipmentAlarm Package: femto.nbicreatedeviceavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi createDevice.avg		
Remedial action: Not available		

Table 23-379 nbicreatesingledeviceoperation

Alarm	Attributes	Applicable major release
Name: nbicreatesingledeviceoperation (6399) Type: equipmentAlarm Package: femto.nbicreatesingledeviceoperation Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi createSingleDeviceOperation		
Remedial action: Not available		

Table 23-380 nbicreatesingledeviceoperationavg

Alarm	Attributes	Applicable major release
Name: nbicreatesingledeviceoperationavg (6400) Type: equipmentAlarm Package: femto.nbicreatesingledeviceoperationavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi createSingleDeviceOperation.avg		
Remedial action: Not available		

Table 23-381 nbicreatesingledeviceoperationbydeviceguid

Alarm	Attributes	Applicable major release
Name: nbicreatesingledeviceoperationbydeviceguid (6401) Type: equipmentAlarm Package: femto. nbicreatesingledeviceoperationbydeviceguid Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi createSingleDeviceOperationByDeviceGUID		
Remedial action: Not available		

Table 23-382 nbicreatesingledeviceoperationbydeviceguidavg

Alarm	Attributes	Applicable major release
Name: nbicreatesingledeviceopera-tionbydeviceguidavg (6402) Type: equipmentAlarm Package: femto. nbicreatesingledeviceoperationbydeviceguidavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2

Table 23-382 nbicreatesingledeviceoperationbydeviceguidavg (continued)

Alarm	Attributes	Applicable major release
Description: number of nbi createSingleDeviceOperationByDeviceGUID.avg		
Remedial action: Not available		

Table 23-383 nbifinddevicebyguid

Alarm	Attributes	Applicable major release
Name: nbifinddevicebyguid (6403) Type: equipmentAlarm Package: femto.nbifinddevicebyguid Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi findDeviceByGUID		
Remedial action: Not available		

Table 23-384 nbifinddevicebyguidavg

Alarm	Attributes	Applicable major release
Name: nbifinddevicebyguidavg (6404) Type: equipmentAlarm Package: femto.nbifinddevicebyguidavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi findDeviceByGUID.avg		
Remedial action: Not available		

Table 23-385 nbifinddevices

Alarm	Attributes	Applicable major release
Name: nbifinddevices (6405) Type: equipmentAlarm Package: femto.nbifinddevices Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi findDevices		
Remedial action: Not available		

Table 23-386 nbifinddevicesavg

Alarm	Attributes	Applicable major release
Name: nbifinddevicesavg (6406) Type: equipmentAlarm Package: femto.nbifinddevicesavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi findDevices.avg		
Remedial action: Not available		

Table 23-387 nbigetactivealarms

Alarm	Attributes	Applicable major release
Name: nbigetactivealarms (6407) Type: equipmentAlarm Package: femto.nbigetactivealarms Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi getActiveAlarms		
Remedial action: Not available		

Table 23-388 nbigetactivealarmsavg

Alarm	Attributes	Applicable major release
Name: nbigetactivealarmsavg (6408) Type: equipmentAlarm Package: femto.nbigetactivealarmsavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi getActiveAlarms.avg		
Remedial action: Not available		

Table 23-389 nbigetcacheddatamodelparameters

Alarm	Attributes	Applicable major release
Name: nbigetcacheddatamodelparameters (6409) Type: equipmentAlarm Package: femto.nbigetcacheddatamodelparameters Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi getCachedDataModelParameters		
Remedial action: Not available		

Table 23-390 nbigetcacheddatamodelparametersavg

Alarm	Attributes	Applicable major release
Name: nbigetcacheddatamodelparametersavg (6410) Type: equipmentAlarm Package: femto. nbigetcacheddatamodelparametersavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi getCachedDataModelParameters.avg		
Remedial action: Not available		

Table 23-391 nbiinitiateconnectionrequest

Alarm	Attributes	Applicable major release
Name: nbiinitiateconnectionrequest (6411) Type: equipmentAlarm Package: femto.nbiinitiateconnectionrequest Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi initiateConnectionRequest		
Remedial action: Not available		

Table 23-392 nbiinitiateconnectionrequestavg

Alarm	Attributes	Applicable major release
Name: nbiinitiateconnectionrequestavg (6412) Type: equipmentAlarm Package: femto.nbiinitiateconnectionrequestavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi initiateConnectionRequest.avg		
Remedial action: Not available		

Table 23-393 NBIoTLTECell_lteNbIotRrcSctpAssociationFailure

Alarm	Attributes	Applicable major release
Name: NBIoTLTECell_ lteNbIotRrcSctpAssociationFailure (12744) Type: communicationsAlarm Package: femto.NBIoTLTECell_ lteNbIotRrcSctpAssociationFailure Raised on class: femto.NBIoTLTECell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError	Release: • 14.2

Table 23-393 NBIoTLTECell_lteNbIotRrcSctpAssociationFailure (continued)

Alarm	Attributes	Applicable major release
Description: RRC/SCTP association failure alarm. This alarm is triggered by: 1) eNB receives an ErrorInd from MME with Criticality Diagnostics; 2) S1Setup response timer expires and maximum retries exhausted; 3) receive S1Setup Failure from MME and maximum retries exhausted; 4) during S1Setup, SCTP conn failure; 5) SCTP s1 setup req send fails; 6) upon expiration of sctp connection recovery timer; 7) gets sctp shutdown from mme when cell is up.		
Remedial action: Depending on fault condition, the cell may need reboot to recover SCTP association. Look MME IP address in the Additional Text field of this alarm message for SCTP association.		

Table 23-394 NBIoTLTECell_nbCellOperationFailure

Alarm	Attributes	Applicable major release
Name: NBIoTLTECell_nbCellOperationFailure (12971) Type: processingErrorAlarm Package: femto.NBIoTLTECell_ nbCellOperationFailure Raised on class: femto.NBIoTLTECell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • 14.2
Description: This alarm is generated, when internal NB-IOT cell related autonomous operations (like Block/Unblock) fails.		
Remedial action: No action needed from the operator. AP is rebooted by Nokia OAM after 4 hours if NB auto recovery is enabled.		

Table 23-395 NBIoTLTECell_spareNbIotCellAlarm1

Alarm	Attributes	Applicable major release
Name: NBIoTLTECell_spareNbIotCellAlarm1 (12745) Type: processingErrorAlarm Package: femto.NBIoTLTECell_spareNbIotCellAlarm1 Raised on class: femto.NBIoTLTECell	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details		

Table 23-396 NBIoTLTECell_spareNbIotCellAlarm2

Alarm	Attributes	Applicable major release
Name: NBIoTLTECell_spareNbIotCellAlarm2 (12746) Type: processingErrorAlarm Package: femto.NBIoTLTECell_spareNbIotCellAlarm2 Raised on class: femto.NBIoTLTECell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details		

Table 23-397 NBIoTLTECell_spareNbIotCellAlarm3

Alarm	Attributes	Applicable major release
Name: NBIoTLTECell_spareNbIotCellAlarm3 (12747) Type: processingErrorAlarm Package: femto.NBIoTLTECell_spareNbIotCellAlarm3 Raised on class: femto.NBIoTLTECell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details		

Table 23-398 nbiraisealarm

Alarm	Attributes	Applicable major release
Name: nbiraisealarm (6413) Type: equipmentAlarm Package: femto.nbiraisealarm Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi raiseAlarm		
Remedial action: Not available		

Table 23-399 nbiraisealarmavg

Alarm	Attributes	Applicable major release
Name: nbiraisealarmavg (6414) Type: equipmentAlarm Package: femto.nbiraisealarmavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi raiseAlarm.avg		
Remedial action: Not available		

Table 23-400 nbiregisterdevice

Alarm	Attributes	Applicable major release
Name: nbiregisterdevice (6415) Type: equipmentAlarm Package: femto.nbiregisterdevice Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi registerDevice		
Remedial action: Not available		

Table 23-401 nbiregisterdeviceavg

Alarm	Attributes	Applicable major release
Name: nbiregisterdeviceavg (6416) Type: equipmentAlarm Package: femto.nbiregisterdeviceavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi registerDevice.avg		
Remedial action: Not available		

Table 23-402 nbireleasedevice

Alarm	Attributes	Applicable major release
Name: nbireleasedevice (6417) Type: equipmentAlarm Package: femto.nbireleasedevice Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi releaseDevice		
Remedial action: Not available		

Table 23-403 nbireleasedeviceavg

Alarm	Attributes	Applicable major release
Name: nbireleasedeviceavg (6418) Type: equipmentAlarm Package: femto.nbireleasedeviceavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi releaseDevice.avg		
Remedial action: Not available		

Table 23-404 nbireruneventtriggeredpolicy

Alarm	Attributes	Applicable major release
Name: nbireruneventtriggeredpolicy (6419) Type: equipmentAlarm Package: femto.nbireruneventtriggeredpolicy Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi rerunEventTriggeredPolicy		
Remedial action: Not available		

Table 23-405 nbireruneventtriggeredpolicyavg

Alarm	Attributes	Applicable major release
Name: nbireruneventtriggeredpolicyavg (6420) Type: equipmentAlarm Package: femto.nbireruneventtriggeredpolicyavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi rerunEventTriggeredPolicy.avg		
Remedial action: Not available		

Table 23-406 nbiruneventtriggeredpolicies

Alarm	Attributes	Applicable major release
Name: nbiruneventtriggeredpolicies (6421) Type: equipmentAlarm Package: femto.nbiruneventtriggeredpolicies Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi runEventTriggeredPolicies		
Remedial action: Not available		

Table 23-407 nbiruneventtriggeredpoliciesavg

Alarm	Attributes	Applicable major release
Name: nbiruneventtriggeredpoliciesavg (6422) Type: equipmentAlarm Package: femto.nbiruneventtriggeredpoliciesavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi runEventTriggeredPolicies.avg		
Remedial action: Not available		

Table 23-408 nbiupdatedevicebydeviceid

Alarm	Attributes	Applicable major release
Name: nbiupdatedevicebydeviceid (6423) Type: equipmentAlarm Package: femto.nbiupdatedevicebydeviceid Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi updateDeviceByDeviceID		
Remedial action: Not available		

Table 23-409 nbiupdatedevicebydeviceidavg

Alarm	Attributes	Applicable major release
Name: nbiupdatedevicebydeviceidavg (6424) Type: equipmentAlarm Package: femto.nbiupdatedevicebydeviceidavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi updateDeviceByDeviceID.avg		
Remedial action: Not available		

Table 23-410 nbiupdatedevicebyguid

Alarm	Attributes	Applicable major release
Name: nbiupdatedevicebyguid (6425) Type: equipmentAlarm Package: femto.nbiupdatedevicebyguid Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi updateDeviceByGUID		
Remedial action: Not available		

Table 23-411 nbiupdatedevicebyguidavg

Alarm	Attributes	Applicable major release
Name: nbiupdatedevicebyguidavg (6426) Type: equipmentAlarm Package: femto.nbiupdatedevicebyguidavg Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: number of nbi updateDeviceByGUID.avg		
Remedial action: Not available		

Table 23-412 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 14.2

Table 23-412 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 23-413 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 14.2
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 23-414 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 14.2
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		

Table 23-414 NodeDatabaseFallbackDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 23-415 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 14.2
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 23-416 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 14.2
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 23-417 OAM_160

Alarm	Attributes	Applicable major release
Name: OAM_160 (6158) Type: communicationsAlarm Package: femto.OAM_160 Raised on class: femto.FemtoCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: Loss of OAM link between OMC and HNM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-418 OAM_161

Alarm	Attributes	Applicable major release
Name: OAM_161 (6159) Type: qualityOfServiceAlarm Package: femto.OAM_161 Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2
Description: BSR is not operational or the OSI state is degraded		
Remedial action: Check the operationalState and availabilityStatus of the BSR MO on HDM		

Table 23-419 OAM_162

Alarm	Attributes	Applicable major release
Name: OAM_162 (6160) Type: communicationsAlarm Package: femto.OAM_162 Raised on class: femto.FemtoCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: Loss of communication link between WMS and FileServer		
Remedial action: Check the communication link between WMS and FileServer. This notification may be required by Global Product Support for debugging purposes		

Table 23-420 OAM_163

Alarm	Attributes	Applicable major release
Name: OAM_163 (6161) Type: equipmentAlarm Package: femto.OAM_163 Raised on class: femto.Femto	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 14.2
Description: Allocated license issue.		
Remedial action: Check WLM Web GUI to get more information on the current license settings.		

Table 23-421 OAM_164

Alarm	Attributes	Applicable major release
Name: OAM_164 (6162) Type: processingErrorAlarm Package: femto.OAM_164 Raised on class: femto.Femto	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizationError	Release: • 14.2
Description: Self optimization operation not triggerred for the Femto Network Element.		
Remedial action: NA		

Table 23-422 OAM_165

Alarm	Attributes	Applicable major release
Name: OAM_165 (6163) Type: operationalViolation Package: femto.OAM_165 Raised on class: femto.Femto	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 14.2
Description: Self optimization was not successfull for Femto		
Remedial action: NA		

Table 23-423 OAM_222

Alarm	Attributes	Applicable major release
Name: OAM_222 (11161) Type: communicationsAlarm Package: femto.OAM_222 Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystemFailure	Release: • 14.2

Table 23-423 OAM_222 (continued)

Alarm	Attributes	Applicable major release
Description: Loss of OAM link between SCMS and HDM.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 23-424 OAM_225

Alarm	Attributes	Applicable major release
Name: OAM_225 (11162) Type: communicationsAlarm Package: femto.OAM_225 Raised on class: femto.HDMCluster	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The OAMLinkAdministrativeState parameter (HDMCluster object) is set to locked.		
Remedial action: Find out why the OAMLinkAdministrativeState was locked in the first place. Set the OAMLinkAdministrativeState parameter (HDMCluster object) to unlocked.		

Table 23-425 OAM_LCellDown

Alarm	Attributes	Applicable major release
Name: OAM_LCellDown (9624) Type: qualityOfServiceAlarm Package: femto.OAM_LCellDown Raised on class: femto.LCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2
Description: LCell is not operational or the OSI state is degraded		
Raising condition: (('availabilityStatus' NOT EQUAL 'inTest') OR ('operationalState' NOT EQUAL 'enabled'))		
Clearing condition: (('availabilityStatus' EQUAL 'inTest') AND ('operationalState' EQUAL 'enabled'))		
Remedial action: Check the operationalState and availabilityStatus of the LCell MO on HDM		

Table 23-426 OAM_LteCellDown

Alarm	Attributes	Applicable major release
Name: OAM_LteCellDown (9625) Type: qualityOfServiceAlarm Package: femto.OAM_LteCellDown Raised on class: femto.LteCell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 14.2
Description: LteCell is not operational or the OSI state is degraded		

Table 23-426 OAM_LteCellDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('availabilityStatus' NOT EQUAL 'inTest') OR ('operationalState' NOT EQUAL 'enabled'))		
Clearing condition: (('availabilityStatus' EQUAL 'inTest') AND ('operationalState' EQUAL 'enabled'))		
Remedial action: Check the operationalState and availabilityStatus of the LteCell MO on HDM		

Table 23-427 OAM_NBIoTLTECellDown

Alarm	Attributes	Applicable major release
Name: OAM_NBIoTLTECellDown (12748) Type: qualityOfServiceAlarm Package: femto.OAM_NBIoTLTECellDown Raised on class: femto.NBIoTLTECell	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 14.2
Description: NBIoTLTECell is not operational or the OSI state is degraded.		
Raising condition: (('availabilityStatus' NOT EQUAL 'inTest') OR ('operationalState' NOT EQUAL 'enabled'))		
Clearing condition: (('availabilityStatus' EQUAL 'inTest') AND ('operationalState' EQUAL 'enabled'))		
Remedial action: Check the operationalState and availabilityStatus of the NBIoTLTECell MO on HDM.		

Table 23-428 operationresultOverload

Alarm	Attributes	Applicable major release
Name: operationresultOverload (11172) Type: equipmentAlarm Package: femto.operationresultOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for operation result events.		
Remedial action: Threshold exceeds for operation result events		

Table 23-429 osavailableprocessercount

Alarm	Attributes	Applicable major release
Name: osavailableprocessercount (6427) Type: equipmentAlarm Package: femto.osavailableprocessercount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of processer available to os		
Remedial action: Not available		

Table 23-430 oscommittedvirtualmemory

Alarm	Attributes	Applicable major release
Name: oscommittedvirtualmemory (6428) Type: equipmentAlarm Package: femto.oscommittedvirtualmemory Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The Number of committed virtual memory		
Remedial action: Not available		

Table 23-431 oscpuutil

Alarm	Attributes	Applicable major release
Name: oscpuutil (12507) Type: equipmentAlarm Package: femto.oscpuutil Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Current CPU utilization percentage of physical box hosting the current managed server. If the value goes above 90 percent it might be an indication of overloading scenario.		
Remedial action: Not available		

Table 23-432 osfreephysicalmemory

Alarm	Attributes	Applicable major release
Name: osfreephysicalmemory (6429) Type: equipmentAlarm Package: femto.osfreephysicalmemory Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The Number of free memory		
Remedial action: Not available		

Table 23-433 osfreeswapspace

Alarm	Attributes	Applicable major release
Name: osfreeswapspace (6430) Type: equipmentAlarm Package: femto.osfreeswapspace Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Free swap space size		
Remedial action: Not available		

Table 23-434 osmaxfiledescriptor

Alarm	Attributes	Applicable major release
Name: osmaxfiledescriptor (6431) Type: equipmentAlarm Package: femto.osmaxfiledescriptor Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Maximum file secriptor		
Remedial action: Not available		

Table 23-435 osopenfiledescriptor

Alarm	Attributes	Applicable major release
Name: osopenfiledescriptor (6432) Type: equipmentAlarm Package: femto.osopenfiledescriptor Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of open file descriptor		
Remedial action: Not available		

Table 23-436 osprocesscputime

Alarm	Attributes	Applicable major release
Name: osprocesscputime (6433) Type: equipmentAlarm Package: femto.osprocesscputime Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The CPU time		
Remedial action: Not available		

Table 23-437 ostotalphysicalmemory

Alarm	Attributes	Applicable major release
Name: ostotalphysicalmemory (6434) Type: equipmentAlarm Package: femto.ostotalphysicalmemory Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Total Physical memory		
Remedial action: Not available		

Table 23-438 ostotalswapspace

Alarm	Attributes	Applicable major release
Name: ostotalswapspace (6435) Type: equipmentAlarm Package: femto.ostotalswapspace Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Total number of free sawp space		
Remedial action: Not available		

Table 23-439 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 14.2
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 23-440 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 14.2
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 23-441 periodicinformpercentage

Alarm	Attributes	Applicable major release
Name: periodicinformpercentage (6436) Type: equipmentAlarm Package: femto.periodicinformpercentage Raised on class: femto.HDMCluster	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Percentage of periodic informs		
Remedial action: Not available		

Table 23-442 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 14.2
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 23-443 PM_pmAuthenticationError

Alarm	Attributes	Applicable major release
Name: PM_pmAuthenticationError (6168) Type: communicationsAlarm Package: femto.PM_pmAuthenticationError Raised on class: femto.PM	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unauthorizedAccessAttempt	Release: • 14.2
Description: The authentication error when transferring PM files.		
Remedial action: The operator should check SFTP server and related configuration. If the problem persists, contact Nokia customer support		

Table 23-444 PM_pmCommunicationError

Alarm	Attributes	Applicable major release
Name: PM_pmCommunicationError (6169) Type: communicationsAlarm Package: femto.PM_pmCommunicationError Raised on class: femto.PM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • 14.2
Description: Failure to transferring PM files even after retries.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-445 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 14.2
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 23-446 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 14.2
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 23-447 Radio_clockSynchronisationFailure

Alarm	Attributes	Applicable major release
Name: Radio_clockSynchronisationFailure (6195) Type: equipmentAlarm Package: femto.Radio_clockSynchronisationFailure Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised if discipline process fails, i.e. the convergence does not occur within 4 hours of convergence time. The NTP/PTP servers are reachable but the NTP/PTP Client is not in 'synced' state.		
Remedial action: Operator could check configuration and status of NTP server.		

Table 23-448 Radio_freqSynchronisationFailure

Alarm	Attributes	Applicable major release
Name: Radio_freqSynchronisationFailure (8205) Type: equipmentAlarm Package: femto.Radio_freqSynchronisationFailure Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised if no discipline source is available and the oscillator holdover period has been exceeded such that frequency may no longer meet system requirements. (A separate alarm is defined for reporting phase synchronization failure).		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support		

Table 23-449 Radio_gpsServiceUnavailable

Alarm	Attributes	Applicable major release
Name: Radio_gpsServiceUnavailable (8206) Type: equipmentAlarm Package: femto.Radio_gpsServiceUnavailable Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: The fault is raised if the GPS timing signal is not available.		
Remedial action: Check if GPS is connected		

Table 23-450 Radio_nlRfFailure

Alarm	Attributes	Applicable major release
Name: Radio_nlRfFailure (8207) Type: equipmentAlarm Package: femto.Radio_nlRfFailure Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The Network Listen hardware has a receive path failure.		

Table 23-450 Radio_nlRfFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: This is generally due to a hardware failure, the MS MCI may need to be replaced. contact Nokia customer support.		

Table 23-451 Radio_ntpServiceUnavailable

Alarm	Attributes	Applicable major release
Name: Radio_ntpServiceUnavailable (6196) Type: equipmentAlarm Package: femto.Radio_ntpServiceUnavailable Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised if NTP servers are initially not reachable within 5 minutes and verification of calibration value is impossible in this timeframe. This fault is also raised if the discipline process fails due to the NTP servers being unreachable. The nature of the failure will be provided in the additional text.		
Remedial action: Check whether primary/secondary NTP servers are reachable		

Table 23-452 Radio_oscillatorAdjustFail

Alarm	Attributes	Applicable major release
Name: Radio_oscillatorAdjustFail (8208) Type: equipmentAlarm Package: femto.Radio_oscillatorAdjustFail Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The timing oscillator has reached its adjustment limit.		
Remedial action: This is a hardware failure and the MS MCI must be replaced.		

Table 23-453 Radio_otaServiceUnavailable

Alarm	Attributes	Applicable major release
Name: Radio_otaServiceUnavailable (13001) Type: equipmentAlarm Package: femto.Radio_otaServiceUnavailable Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised if the discipline process fails due to OTA sync source not available		
Remedial action: Check whether proper macro neighbour frequencies are configured for OTA sync		

Table 23-454 Radio_outOfOperatingCondition

Alarm	Attributes	Applicable major release
Name: Radio_outOfOperatingCondition (6197) Type: equipmentAlarm Package: femto.Radio_outOfOperatingCondition Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: This fault is raised if out of operating condition is detected. It is related to critical hardware checks on LightRadio Metro Cells, for example power amplifier 28V supply and current monitoring on LightRadio 2100 and 1900 Metro Outdoor Cells.		
Remedial action: This fault is related to critical hardware failure. If the problem persists, contact Nokia customer support.		

Table 23-455 Radio_overTemperature

Alarm	Attributes	Applicable major release
Name: Radio_overTemperature (6198) Type: environmentalAlarm Package: femto.Radio_overTemperature Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2
Description: The temperature is over the specified limit. For Multi-Standard MS-HC v1 boards, if zone 0 to 7 sensors cross the threshold temperature of 98 C, the alarm would be raised with the additional text WARNING and if PA sensors cross the threshold temperature of 90 C, the alarm would be raised with the additional text CRITICAL		
Remedial action: The alarm will be cleared by the Small Cell once the temperature has fallen below the specified limit. The operator should investigate why the temperature rose over the limit. If the problem persists, contact Nokia customer support.		

Table 23-456 Radio_phaseSynchronisationFailure

Alarm	Attributes	Applicable major release
Name: Radio_phaseSynchronisationFailure (8498) Type: equipmentAlarm Package: femto.Radio_phaseSynchronisationFailure Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingProblem	Release: • 14.2
Description: This fault is raised if the current phase error may exceed the operating limits of any currently provisioned phase-dependent functions.		
Remedial action: Operator should check status of phase reference sources (GPS or PTP (future)).		

Table 23-457 Radio_rxDiversityMalfunction

Alarm	Attributes	Applicable major release
Name: Radio_rxDiversityMalfunction (6199) Type: equipmentAlarm Package: femto.Radio_rxDiversityMalfunction Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Raised when one of the two Rx path fails when receive diversity is active.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-458 Radio_rxMalfunction

Alarm	Attributes	Applicable major release
Name: Radio_rxMalfunction (6200) Type: equipmentAlarm Package: femto.Radio_rxMalfunction Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: Malfunction in the radio receiver.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-459 Radio_spareRadioAlarm1

Alarm	Attributes	Applicable major release
Name: Radio_spareRadioAlarm1 (8209) Type: processingErrorAlarm Package: femto.Radio_spareRadioAlarm1 Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 1		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-460 Radio_spareRadioAlarm2

Alarm	Attributes	Applicable major release
Name: Radio_spareRadioAlarm2 (8210) Type: processingErrorAlarm Package: femto.Radio_spareRadioAlarm2 Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 2		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-461 Radio_spareRadioAlarm3

Alarm	Attributes	Applicable major release
Name: Radio_spareRadioAlarm3 (8211) Type: processingErrorAlarm Package: femto.Radio_spareRadioAlarm3 Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: Spare alarm 3		
Remedial action: Refer to customer documentation for alarm details.		

Table 23-462 Radio_txMalfunction

Alarm	Attributes	Applicable major release
Name: Radio_txMalfunction (6201) Type: equipmentAlarm Package: femto.Radio_txMalfunction Raised on class: femto.Radio	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 14.2
Description: The Radio has failed to activate the transmitter, or malfunction in the radio transmitter.		
Remedial action: If the problem persists, contact Nokia customer support		

Table 23-463 Radio_underTemperature

Alarm	Attributes	Applicable major release
Name: Radio_underTemperature (6202) Type: environmentalAlarm Package: femto.Radio_underTemperature Raised on class: femto.Radio	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • 14.2
Description: The temperature is below the specified limit.		
Remedial action: The alarm will be cleared by the Small Cell once the temperature has risen above the specified limit. The operator should investigate the reason for the excessively low temperature. If the problem persists, contact Nokia customer support.		

Table 23-464 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 14.2
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		

Table 23-464 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 23-465 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 14.2
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 23-466 reachabledevicecount

Alarm	Attributes	Applicable major release
Name: reachabledevicecount (6437) Type: equipmentAlarm Package: femto.reachabledevicecount Raised on class: femto.HDMCluster	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Count of reachable devices		
Remedial action: Not available		

Table 23-467 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 14.2

Table 23-467 ReconfigFailure (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 23-468 resyncEventsOverload

Alarm	Attributes	Applicable major release
Name: resyncEventsOverload (11173) Type: equipmentAlarm Package: femto.resyncEventsOverload Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Threshold exceeds for Resync events.		
Raising condition: (('Resync Event OverLoad' EQUAL 'true'))		
Clearing condition: (('Resync Event OverLoad' EQUAL 'false'))		
Remedial action: Threshold exceeds for resync events		

Table 23-469 RFTrace_rfTraceDedicatedFailure

Alarm	Attributes	Applicable major release
Name: RFTrace_rfTraceDedicatedFailure (6189) Type: operationalViolation Package: femto.RFTrace_rfTraceDedicatedFailure Raised on class: femto.RFTrace	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised during RF Trace operation if all dedicated measurement (excluding HSDPA and EDCH) configurations are failed.		
Remedial action: This alarm does not require operator intervention. It will affect only RF Trace operation as it will blocked because of the failure. If the problem persists, contact Nokia customer support.		

Table 23-470 RFTrace_rfTraceHsdpaFailure

Alarm	Attributes	Applicable major release
Name: RFTrace_rfTraceHsdpaFailure (6190) Type: operationalViolation Package: femto.RFTrace_rfTraceHsdpaFailure Raised on class: femto.RFTrace	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is raised during RF Trace operation if all HSDPA measurement configurations are failed.		
Remedial action: This alarm does not require operator intervention. It will affect only RF Trace operation as it will blocked because of the failure. If the problem persists, contact Nokia customer support.		

Table 23-471 RFTrace_rfTraceRssiFailure

Alarm	Attributes	Applicable major release
Name: RFTrace_rfTraceRssiFailure (8497) Type: operationalViolation Package: femto.RFTrace_rfTraceRssiFailure Raised on class: femto.RFTrace	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • 14.2
Description: This fault is raised during RF Trace operation if RSSI data collection fails.		
Remedial action: The alarm is cleared when the operator unlocks (administrative state) the RFTrace MO.		

Table 23-472 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 14.2
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 23-473 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 14.2
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 23-474 SCTPASSOC_associationEstablishmentFailure

Alarm	Attributes	Applicable major release
Name: SCTPASSOC_associationEstablishmentFailure (6203) Type: communicationsAlarm Package: femto.SCTPASSOC_ associationEstablishmentFailure Raised on class: femto.SCTPASSOC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised after the number of INIT retries configured by maxInitRetransmits has failed. After the fault is raised there will be further retries after maxDelaySctpReEst delay		
Remedial action: The alarm is cleared by the Small Cell once the SCTP association is made. If the problem persists, contact Nokia customer support.		

Table 23-475 SCTPASSOC_sctpAssocAssociationDownAlarm

Alarm	Attributes	Applicable major release
Name: SCTPASSOC_ sctpAssocAssociationDownAlarm (6204) Type: communicationsAlarm Package: femto.SCTPASSOC_ sctpAssocAssociationDownAlarm Raised on class: femto.SCTPASSOC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This fault is raised when all SCTP associations with the BSG are down.		
Remedial action: The operator should check the configuration of BSG IP address and whether the BSG is operational. If the problem persists, contact Nokia customer support.		

Table 23-476 SCTPASSOC_sctpAssocDnsFailure

Alarm	Attributes	Applicable major release
Name: SCTPASSOC_sctpAssocDnsFailure (6205) Type: communicationsAlarm Package: femto.SCTPASSOC_sctpAssocDnsFailure Raised on class: femto.SCTPASSOC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: This fault is sent when link failure is detected when no response is received to DNS messages attempting to resolve the FGW FQDN. This maybe caused by timeout or a protocol error.		
Remedial action: Operator could check configuration of BSG FQDN, ensure operator DNS servers are provisioned in FBSR at IPsec tunnel establishment, ensure operator DNS servers are reachable from FBSR, and ensure operator DNS servers contain Resource Records for the BSG FQDN.		

Table 23-477 SCTPASSOC_unstableSCTPAssociation

Alarm	Attributes	Applicable major release
Name: SCTPASSOC_unstableSCTPAssociation (8499) Type: communicationsAlarm Package: femto.SCTPASSOC_unstableSCTPAssociation Raised on class: femto.SCTPASSOC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 14.2
Description: This fault is raised if the SCTP association to the SCGW has been unstable with many short term interruptions- Probable Cause: communicationsSubsystemFailure		
Remedial action: Operator can investigate the stability of the backhaul links between the BSR and SCGW		

Table 23-478 SDM_dbDownloadFailure

Alarm	Attributes	Applicable major release
Name: SDM_dbDownloadFailure (6209) Type: processingErrorAlarm Package: femto.SDM_dbDownloadFailure Raised on class: femto.SDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This fault is created when the database download fails.		
Remedial action: This alarm does not require operator intervention. If the problem persists, contact Nokia customer support.		

Table 23-479 SDM_suActivationFailure

Alarm	Attributes	Applicable major release
Name: SDM_suActivationFailure (6210) Type: processingErrorAlarm Package: femto.SDM_suActivationFailure Raised on class: femto.SDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This fault is created when activation of a software image fails.		
Remedial action: The alarm will be cleared by the Small Cell once the software activation has succeeded. If the problem persists, contact Nokia customer support		

Table 23-480 SDM_suDownloadFailure

Alarm	Attributes	Applicable major release
Name: SDM_suDownloadFailure (6211) Type: processingErrorAlarm Package: femto.SDM_suDownloadFailure Raised on class: femto.SDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This fault is created when download of a software image fails.		
Remedial action: The alarm will be cleared by the Small Cell when the database has been successfully downloaded. If the problem persists, contact Nokia customer support		

Table 23-481 SDM_toneFileCorrupt

Alarm	Attributes	Applicable major release
Name: SDM_toneFileCorrupt (6212) Type: processingErrorAlarm Package: femto.SDM_toneFileCorrupt Raised on class: femto.SDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: A downloaded tone file has invalid format.		
Remedial action: Check the tone file and retry the download.If the problem persists, contact Nokia customer support.		

Table 23-482 SDM_toneFileDownloadFailure

Alarm	Attributes	Applicable major release
Name: SDM_toneFileDownloadFailure (6213) Type: processingErrorAlarm Package: femto.SDM_toneFileDownloadFailure Raised on class: femto.SDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 14.2
Description: This fault is created when download of a tone file fails.		

Table 23-482 SDM_toneFileDownloadFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Retry the download. If the problem persists, contact Nokia customer support		

Table 23-483 socketcount

Alarm	Attributes	Applicable major release
Name: socketcount (6438) Type: equipmentAlarm Package: femto.socketcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of socket		
Remedial action: Not available		

Table 23-484 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 14.2
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 23-485 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 14.2
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 23-485 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 23-486 threadidlecount

Alarm	Attributes	Applicable major release
Name: threadidlecount (6439) Type: equipmentAlarm Package: femto.threadidlecount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of idel threads		
Remedial action: Not available		

Table 23-487 threadpendingrequestcount

Alarm	Attributes	Applicable major release
Name: threadpendingrequestcount (6440) Type: equipmentAlarm Package: femto.threadpendingrequestcount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of thread in pending request state		
Remedial action: Not available		

Table 23-488 threadqueuelength

Alarm	Attributes	Applicable major release
Name: threadqueuelength (6441) Type: equipmentAlarm Package: femto.threadqueuelength Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of thread queue		
Remedial action: Not available		

Table 23-489 threadstandbycount

Alarm	Attributes	Applicable major release
Name: threadstandbycount (6442) Type: equipmentAlarm Package: femto.threadstandbycount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: The number of thread in stand by state.		
Remedial action: Not available		

Table 23-490 threadthroughput

Alarm	Attributes	Applicable major release
Name: threadthroughput (6443) Type: equipmentAlarm Package: femto.threadthroughput Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Thread throughput		
Remedial action: Not available		

Table 23-491 threadtotalcount

Alarm	Attributes	Applicable major release
Name: threadtotalcount (6444) Type: equipmentAlarm Package: femto.threadtotalcount Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Total number of Threads		
Remedial action: Not available		

Table 23-492 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 14.2

Table 23-492 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 23-493 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 14.2
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 23-494 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw.TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 14.2
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 23-495 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 14.2
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 23-496 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 14.2

Table 23-496 UnmanageFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 23-497 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 14.2
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 23-498 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 14.2
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 23-499 UpgradeRulesFileAlarm

Alarm	Attributes	Applicable major release
Name: UpgradeRulesFileAlarm (9019) Type: processingErrorAlarm Package: femto.UpgradeRulesFileAlarm Raised on class: femto.SmallCellProfileUpgradeActions	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • 14.2
Description: The alarm is raised when there is any issue with the Upgrade Rules File.		
Remedial action: Please provide a valid Upgrade Rules File		

Table 23-500 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 14.2
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 23-501 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 14.2
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 23-502 userlockouttotalcount

Alarm	Attributes	Applicable major release
Name: userlockouttotalcount (6445) Type: equipmentAlarm Package: femto.userlockouttotalcount Raised on class: femto.HDMCluster	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 14.2
Description: Indicates how many user locking out process is executed on the current server		
Remedial action: Not available		

Table 23-503 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 14.2
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 23-504 WiFi_wifiNoSignalDetected

Alarm	Attributes	Applicable major release
Name: WiFi_wifiNoSignalDetected (6247) Type: communicationsAlarm Package: femto.WiFi_wifiNoSignalDetected Raised on class: femto.WiFi	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 14.2
Description: This fault is raised if signal of link status is not detected on the Wi-Fi Ethernet port.		
Remedial action: Check whether Wi-Fi AP is attached to the main box of LightRadio MCOs		

Table 23-505 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 14.2
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

24 9471 WMM

24.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 24-1 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 24-2 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 24-3 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 24-4 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 24-5 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 24-6 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 24-7 Connected2GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Connected2GUEsExceeded (5041) Type: communicationsAlarm Package: ltemme.Connected2GUEsExceeded Raised on class: ltemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of Connected 2G UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('2G Connected UEs Threshold' NOT EQUAL '0L') AND ('2G Connected UEs' > '2G Connected UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-8 Connected3GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Connected3GUEsExceeded (5042) Type: communicationsAlarm Package: Itemme.Connected3GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of Connected 3G UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('3G Connected UEs Threshold' NOT EQUAL '0L') AND ('3G Idle UEs' > '3G Connected UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-9 Connected4GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Connected4GUEsExceeded (5043) Type: communicationsAlarm Package: Itemme.Connected4GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of 4G Connected UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('4G Connected UEs Threshold' NOT EQUAL '0L') AND ('4G Connected UEs' > '4G Connected UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-10 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 24-11 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 24-12 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 24-13 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 24-14 criticalErrorAlarm (ltemme)

Alarm	Attributes	Applicable major release
Name: criticalErrorAlarm (3681) Type: communicationsAlarm Package: ltemme.criticalErrorAlarm Raised on class: ltemme.MmeInstance	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MmeInternalProcessingError	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when receiving critical-error message from the network element's NetConf interface. The operator must connect to the network element using its CLI interface and verify the consistency of the network element's database and configuration and then do a full node resync once the manual intervention has been completed.		
Remedial action: The operator must connect to the network element (MME) using its CLI interface and verify the consistency of the network element's database and configuration and then do a full node resync once the manual intervention has been completed.		

Table 24-15 Deregistered4GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Deregistered4GUEsExceeded (5044) Type: communicationsAlarm Package: ltemme.Deregistered4GUEsExceeded Raised on class: ltemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of 4G Deregistered UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('4G Deregistered UEs Threshold' NOT EQUAL '0L') AND ('4G Deregistered UEs' > '4G Deregistered UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-16 EPSPeerLocked

Alarm	Attributes	Applicable major release
Name: EPSPeerLocked (3747) Type: communicationsAlarm Package: lte.EPSPeerLocked Raised on class: lte.AbstractMmeEpsPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerLocked	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an EPS Peer link goes into a locked state. The alarm clears when the EPS Peer Link changes to an unlocked state.		
Raising condition: (('Administrative State' EQUAL 'Locked'))		
Clearing condition: (('Administrative State' EQUAL 'Unlocked'))		
Remedial action: Informational: The EPS Peer has been manually locked.		

Table 24-17 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 24-18 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 24-19 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 24-20 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 24-21 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 24-22 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 24-23 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 24-24 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 24-25 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 24-26 Idle2GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Idle2GUEsExceeded (5045) Type: communicationsAlarm Package: Itemme.Idle2GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of Idle 2G UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('2G Idle UEs Threshold' NOT EQUAL '0L') AND ('2G Idle UEs' > '2G Idle UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-27 Idle3GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Idle3GUEsExceeded (5046) Type: communicationsAlarm Package: Itemme.Idle3GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of Idle 3G UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('3G Idle UEs Threshold' NOT EQUAL '0L') AND ('3G Idle UEs' > '3G Idle UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-28 Idle4GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Idle4GUEsExceeded (5047) Type: communicationsAlarm Package: Itemme.Idle4GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of 4G Idle UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('4G Idle UEs Threshold' NOT EQUAL '0L') AND ('4G Idle UEs' > '4G Idle UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-29 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 24-30 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 24-31 maintenanceStateAlarm

Alarm	Attributes	Applicable major release
Name: maintenanceStateAlarm (4812) Type: operationalViolation Package: ltemme.maintenanceStateAlarm Raised on class: ltemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: WmmMaintenanceState	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when the 9471 WMM is put into maintenance state as part of a software upgrade. While the 9471 WMM is in maintenance mode, 5620 SAM will not process any notifications other than alarms and PM file notifications. In addition, 5620 SAM will not trigger full node resyncs when it receives a Cold Start trap, when it detects that the 9471 WMM has rebooted, or when it detects that the software version of the 9471 WMM has changed. Once the 9471 WMM goes out of maintenance state, 5620 SAM will trigger a full node resync.		
Raising condition: ('Maintenance State' EQUAL 'True')		
Clearing condition: ('Maintenance State' EQUAL 'False')		
Remedial action: Informational - no corrective action required.		

Table 24-32 netconfEventReplayFailure

Alarm	Attributes	Applicable major release
Name: netconfEventReplayFailure (5389) Type: communicationsAlarm Package: ltemme.netconfEventReplayFailure Raised on class: ltemme.MmeInstance	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MmeInternalProcessingError	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: Replay of the NETCONF notification event buffer has failed and 5620 SAM is no longer attempting to replay old events. Any Performance Measurement Statistics files that 5620 SAM was trying to replay must be manually retrieved from the 9471 WMM. The additionalText field of the alarm displays the timestamp of the last successful NETCONF notification that 5620 SAM has processed after server startup. If the additionalText field is empty, we have not processed any NETCONF notifications since the 5620 SAM started and any missing files need to be manually retrieved from the 9471 WMM. New NETCONF event notifications are still processed as normal.		
Remedial action: Replay of the NETCONF notification event buffer has failed and 5620 SAM is no longer attempting to replay old events. Any Performance Measurement Statistics files that 5620 SAM was trying to replay must be manually retrieved from the 9471 WMM. The additionalText field of the alarm displays the timestamp of the last successful NETCONF notification that 5620 SAM has processed after server startup. If the additionalText field is empty, we have not processed any NETCONF notifications since the 5620 SAM started and any missing files need to be manually retrieved from the 9471 WMM. New NETCONF event notifications are still processed as normal.		

Table 24-33 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 24-34 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 24-35 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 24-36 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 24-37 partialSupportAlarm

Alarm	Attributes	Applicable major release
Name: partialSupportAlarm (9566) Type: operationalViolation Package: ltemme.partialSupportAlarm Raised on class: ltemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: WmmPartialSupport	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when the 9471 WMM is running a version of software only partially supported by 5620 SAM. With such a version of 9471 WMM, 5620 SAM only supports alarms and their associated objects as well as PM file collection. No configuration or related operations are supported from 5620 SAM. It will not be possible to upgrade 5620 SAM unless all partially supported 9471 WMM nodes are unmanaged.		
Raising condition: ('Partial Support' EQUAL 'true')		
Remedial action: Informational - no corrective action required.		

Table 24-38 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 24-39 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 24-40 RcaAuditAfterNEUpgradeStatus

Alarm	Attributes	Applicable major release
Name: RcaAuditAfterNEUpgradeStatus (5124) Type: configurationAlarm Package: netw.RcaAuditAfterNEUpgradeStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: rcaAuditStatusAfterNEUpgrade	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM detects an NE software version upgrade and RCA audit performed.		
Remedial action: Information - Check audit results for details		

Table 24-41 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 24-42 Registered4GUEsExceeded

Alarm	Attributes	Applicable major release
Name: Registered4GUEsExceeded (5048) Type: communicationsAlarm Package: Itemme.Registered4GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of 4G Registered UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('4G Registered UEs Threshold' NOT EQUAL '0L') AND ('4G Registered UEs' > '4G Registered UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-43 RegisteredIdle4GUEsExceeded

Alarm	Attributes	Applicable major release
Name: RegisteredIdle4GUEsExceeded (5049) Type: communicationsAlarm Package: Itemme.RegisteredIdle4GUEsExceeded Raised on class: Itemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of 4G Registered Idle UEs exceeds the threshold that has been set by the operator.		
Raising condition: (('4G Registered Idle UEs Threshold' NOT EQUAL '0L') AND ('4G Registered Idle UEs' > '4G Registered Idle UEs Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-44 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 24-45 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 24-46 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 24-47 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 24-48 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 24-49 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 24-50 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 24-51 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 24-52 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 24-53 VNFCAutoHealFailed

Alarm	Attributes	Applicable major release
Name: VNFCAutoHealFailed (9632) Type: configurationAlarm Package: nfv.VNFCAutoHealFailed Raised on class: nfv.VNFComponent	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: vmRebootFailed	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the Auto Heal operation on a given VNF Component fails		
Remedial action: SAM was unable to auto heal the target host residing on the VNF Component. Please contact your Nokia support representative for further assistance.		

Table 24-54 WmmATCA_AggregatePowerSensor

Alarm	Attributes	Applicable major release
Name: WmmATCA_AggregatePowerSensor (4171) Type: mmeAlarm Package: ltemme.WmmATCA_AggregatePowerSensor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The aggregate power sensor alarm provides a summary status of all power related conditions adversely affecting a resource. When this alarm occurs, in most cases, there will be another power related alarm that provides more details about the exact resource power sensor that is reporting the condition. From the MI GUI, alarms on a resource may be retrieved by selecting the managed object for that resource and then selecting the right-click operation to display related alarms.		
Remedial action: Investigate all other temperature and power related alarms on the resource and follow those alarms fault recovery procedures. Once all of these related alarms are cleared, this alarm will clear.		

Table 24-55 WmmATCA_AggregateTemperatureSensor

Alarm	Attributes	Applicable major release
Name: WmmATCA_AggregateTemperatureSensor (4172) Type: mmeAlarm Package: ltemme.WmmATCA_AggregateTemperatureSensor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The aggregate temperatures sensor alarm provides a summary status of all temperature related conditions adversely affecting a resource. When this alarm occurs, in most cases, there will be another temperature related alarm that provides more details about the exact resource temperature sensor that is reporting the condition. From the MI GUI, alarms on a resource may be retrieved by selecting the managed object for that resource and then selecting the right-click operation to display related alarms.		
Remedial action: Investigate all other temperature and power related alarms on the resource and follow those alarms fault recovery procedures. Once all of these related alarms are cleared, this alarm will clear.		

Table 24-56 WmmATCA_BoardPower

Alarm	Attributes	Applicable major release
Name: WmmATCA_BoardPower (4173) Type: mmeAlarm Package: ltemme.WmmATCA_BoardPower Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A board is either in the inactive or not present state. This means that the board has been powered down.		
Remedial action: Verify that the blade is powered on. This can be performed remotely using CLI on the shelf manager or locally by observing specific LEDs and their status\nVerify that the blade is seated correctly in the chassis. Try to re-seat the blade in the chassis.\nReplace the blade if necessary, refer to FRU procedure. Contact your Nokia support representative.		

Table 24-57 WmmATCA_CPLDState

Alarm	Attributes	Applicable major release
Name: WmmATCA_CPLDState (4174) Type: mmeAlarm Package: ltemme.WmmATCA_CPLDState Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a change in the redundancy status of the shelf management cards. The specific problem of the alarm contains the specific redundancy state of the shelf management card.		
Remedial action: Verify that the shelf management card is inserted properly.\nIf the shelf management card is inserted, reseat the shelf management card\nIf reseating the shelf management card does not correct the problem, replace the shelf management card		

Table 24-58 WmmATCA_DS75Temperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_DS75Temperature (4175) Type: mmeAlarm Package: ltemme.WmmATCA_DS75Temperature Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-58 WmmATCA_DS75Temperature (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the AMC (Advanced Mezzanine Card) temperature monitoring sensor has detected a threshold being crossed.		
Remedial action: There is a condition in which this alarm, with minor severity, is being erroneously reported by the hardware, so ignore any minor alarms pertaining to this sensor.\nCheck if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-59 WmmATCA_ExhaustTemp

Alarm	Attributes	Applicable major release
Name: WmmATCA_ExhaustTemp (4176) Type: mmeAlarm Package: Itemme.WmmATCA_ExhaustTemp Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the ASS7BF AMC (Advanced Mezzanine Card) temperature monitoring sensor has detected a threshold being crossed.		
Remedial action: There is a condition in which this alarm, with minor severity, is being erroneously reported by the hardware, so ignore any minor alarms pertaining to this sensor.\nCheck if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-60 WmmATCA_FanSpeed

Alarm	Attributes	Applicable major release
Name: WmmATCA_FanSpeed (4178) Type: mmeAlarm Package: Itemme.WmmATCA_FanSpeed Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that a fan's speed has crossed a threshold.		

Table 24-60 WmmATCA_FanSpeed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the faulty fan unit according to the appropriate replacement procedure.		

Table 24-61 WmmATCA_FanTrayPresence

Alarm	Attributes	Applicable major release
Name: WmmATCA_FanTrayPresence (4179) Type: mmeAlarm Package: ltemme.WmmATCA_FanTrayPresence Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that one of the fan trays is not present in the chassis. The fan tray in question will be identified in the additonalText field of the alarm.		
Remedial action: Insert the fan tray.		

Table 24-62 WmmATCA_FanTraysFRU

Alarm	Attributes	Applicable major release
Name: WmmATCA_FanTraysFRU (4180) Type: mmeAlarm Package: ltemme.WmmATCA_FanTraysFRU Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a problem with one or more of the fan trays.		
Remedial action: Verify that all Fan Trays are properly seated in the chassis.\nVerify that the type of Fan Trays are compatible. Contact your Nokia support representative if incompatible.\nVerify that the cooling parameters are set correctly. Contact your Nokia support representative to adjust parameters.		

Table 24-63 WmmATCA_FilterPresence

Alarm	Attributes	Applicable major release
Name: WmmATCA_FilterPresence (4181) Type: mmeAlarm Package: ltemme.WmmATCA_FilterPresence Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A filter is not present in the chassis. The additional text field of the alarm will indicate which filter is not present.		
Remedial action: Insert the filter that is not present.		

Table 24-64 WmmATCA_FPGATemp

Alarm	Attributes	Applicable major release
Name: WmmATCA_FPGATemp (4177) Type: mmeAlarm Package: ltemme.WmmATCA_FPGATemp Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the DCI AMC (Advanced Mezzanine Card) FPGA Temp monitoring sensor has detected a threshold being crossed. This indicates there is a problem with the die temperature of the DCI FPGA.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-65 WmmATCA_I2CLocalBus

Alarm	Attributes	Applicable major release
Name: WmmATCA_I2CLocalBus (4182) Type: mmeAlarm Package: Itemme.WmmATCA_I2CLocalBus Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm reports an abnormal condition in the hardware state of the I2C Local Bus.		
Remedial action: If the condition does not clear, contact your Nokia support representative		

Table 24-66 WmmATCA_InletTemp

Alarm	Attributes	Applicable major release
Name: WmmATCA_InletTemp (4184) Type: mmeAlarm Package: Itemme.WmmATCA_InletTemp Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the AMC (Advanced Mezzanine Card) Inlet Temp monitoring sensor at the upper edge of the AMC has detected a threshold being crossed.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-67 WmmATCA_IPMBLink

Alarm	Attributes	Applicable major release
Name: WmmATCA_IPMBLink (4183) Type: mmeAlarm Package: Itemme.WmmATCA_IPMBLink Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a problem with the IPMB(Intelligent Platform Management Bus) Link between the shelf manager and the board. This alarm may be reported by the shelf manager for the portion of the link that it monitors, or by the board for the portion of the link it monitors.		
Remedial action: If the Link has been manually disabled, try to enable the link from the active shelf manager card with the command, 'clia setipmbstate <IPMB address> [AB] 1'.\nIf the board is reporting a link failure, replace the board.\nIf the shelf is reporting a link failure, replace the shelf management card.\nIf replacing the board and shelf management card do not solve the problem, replace the shelf. Contact your Nokia support representative.		

Table 24-68 WmmATCA_LM75Temperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_LM75Temperature (4185) Type: mmeAlarm Package: Itemme.WmmATCA_LM75Temperature Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a temperature problem with a board.		
Remedial action: There is a condition in which this alarm, with minor severity, is being erroneously reported by the hardware, so ignore any minor alarms pertaining to this sensor.\nCheck if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-69 WmmATCA_LM83Temperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_LM83Temperature (4186) Type: mmeAlarm Package: ltemme.WmmATCA_LM83Temperature Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a temperature problem with a board. There are 5 LM83 sensors(LM83_1 Local,LM83_1 DBG,LM83_1 BASE,LM83_1 LSI,LM83_2 Local) that monitor the temperature of the board.		
Remedial action: There is a condition in which this alarm, with minor severity, is being erroneously reported by the hardware, so ignore any minor alarms pertaining to this sensor.\nCheck if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-70 WmmATCA_LMeUC75Temperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_LMeUC75Temperature (4188) Type: mmeAlarm Package: ltemme.WmmATCA_LMeUC75Temperature Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the ASS7NB AMC (Advanced Mezzanine Card) temperature monitoring sensor has detected a threshold being crossed.		
Remedial action: There is a condition in which this alarm, with minor severity, is being erroneously reported by the hardware, so ignore any minor alarms pertaining to this sensor.\nCheck if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-71 WmmATCA_LMeUC75TopRig

Alarm	Attributes	Applicable major release
Name: WmmATCA_LMeUC75TopRig (4404) Type: mmeAlarm Package: ltemme.WmmATCA_LMeUC75TopRig Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the ASS7BN AMC (Advanced Mezzanine Card) temperature monitoring sensor has detected a threshold being crossed.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-72 WmmATCA_LocalTemperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_LocalTemperature (4189) Type: mmeAlarm Package: ltemme.WmmATCA_LocalTemperature Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a temperature problem with a board.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-73 WmmATCA_m48vSensor

Alarm	Attributes	Applicable major release
Name: WmmATCA_m48vSensor (4198) Type: mmeAlarm Package: ltemme.WmmATCA_m48vSensor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a problem with the -48V shelf power supply A and/or B feeds.		
Remedial action: Check the top rack power distribution unit's LED and circuit breakers.\nReplace the faulty power supply according to the appropriate replacement procedures.\nIf the problem persists, contact your Nokia support representative.		

Table 24-74 WmmATCA_MMCTemp

Alarm	Attributes	Applicable major release
Name: WmmATCA_MMCTemp (4190) Type: mmeAlarm Package: ltemme.WmmATCA_MMCTemp Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the DCI AMC (Advanced Mezzanine Card) MMC Temp monitoring sensor has detected a threshold being crossed. This indicates there is a problem with the die temperature of the MMC FPGA.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-75 WmmATCA_OcteonTemperature

Alarm	Attributes	Applicable major release
Name: WmmATCA_OcteonTemperature (4191) Type: mmeAlarm Package: ltemme.WmmATCA_OcteonTemperature Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a temperature problem with the Octeon module.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-76 WmmATCA_OutletTemp

Alarm	Attributes	Applicable major release
Name: WmmATCA_OutletTemp (4192) Type: mmeAlarm Package: ltemme.WmmATCA_OutletTemp Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the AMC (Advanced Mezzanine Card) Outlet Temp monitoring sensor at the lower edge of the AMC has detected a threshold being crossed.		
Remedial action: Check if there are other alarms that could explain the rise in temperature, especially fan alarms. If there are, troubleshoot these alarms first.\nCheck that the room air conditioning system is operating properly.\nCheck that the fan units of the suspect chassis are operating correctly. If they are not, replace the fan units according to the replacement procedure.\nIf fans are operating properly and if there is no other alarm, replace faulty FRU according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-77 WmmATCA_PayloadCurrent

Alarm	Attributes	Applicable major release
Name: WmmATCA_PayloadCurrent (4193) Type: mmeAlarm Package: ltemme.WmmATCA_PayloadCurrent Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a current problem on a board, resulting from the Payload Amps sensor threshold being crossed.		
Remedial action: Check if other cards in the chassis have a similar alarm. If this is the case, there may be a problem with the power supply unit(s).\nReplace the faulty card according to the appropriate replacement procedure.\nReplace the interface unit located behind the faulty card according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-78 WmmATCA_PayloadVoltage

Alarm	Attributes	Applicable major release
Name: WmmATCA_PayloadVoltage (4194) Type: mmeAlarm Package: ltemme.WmmATCA_PayloadVoltage Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a voltage problem with a board.		
Remedial action: Check if all of the cards in the chassis have the same alarm. If this is the case, replace the power supply unit(s) according to the appropriate replacement procedure.\nReplace the faulty card according to the appropriate replacement procedure.\nReplace the interface unit located behind the faulty card according to the appropriate replacement procedure.\nIf the problem persists, contact your Nokia support representative.		

Table 24-79 WmmATCA_PowerOk

Alarm	Attributes	Applicable major release
Name: WmmATCA_PowerOk (4195) Type: mmeAlarm Package: ltemme.WmmATCA_PowerOk Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates state of power ok signal from ISPPAC.		
Remedial action: Verify that the blade is powered on.\nVerify that the blade is seated correctly in the chassis. Try to re-seat the blade in the chassis.\nReplace the blade if necessary, refer to FRU procedure. Contact your Nokia support representative.		

Table 24-80 WmmATCA_ShelfFRUs

Alarm	Attributes	Applicable major release
Name: WmmATCA_ShelfFRUs (4196) Type: mmeAlarm Package: ltemme.WmmATCA_ShelfFRUs Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a problem with the shelf FRU information stored in the EEPROMSs (located on the NFATCAV2 back panel and accessed via the I2C local bus). The EEPROMS contents are validated when a shelf manager is initialized as the active shelf manager, and periodically by the active shelf manager.		
Remedial action: A firmware upgrade may be needed, contact your Nokia support representative.		

Table 24-81 WmmATCA_UnexpectedDeact

Alarm	Attributes	Applicable major release
Name: WmmATCA_UnexpectedDeact (4197) Type: mmeAlarm Package: ltemme.WmmATCA_UnexpectedDeact Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-81 WmmATCA_UnexpectedDeact (continued)

Alarm	Attributes	Applicable major release
Description: This sensor reports unexpected deactivation (transition to INACTIVE state) origin. It is asserted		
Remedial action: Look at sensor alarms to see why the card was deactivated and resolve underlying problems.		

Table 24-82 WmmLSS_cardConnectionLost

Alarm	Attributes	Applicable major release
Name: WmmLSS_cardConnectionLost (4199) Type: mmeAlarm Package: Itemme.WmmLSS_cardConnectionLost Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: REM detected a problem with its connectivity to a service member under its control, or a service member has missed a heartbeat to REM.		
Remedial action: Verify the status on the service on the MI GUI. It should be 'Out of Service'. If it is active, or standby hot, with its mate being active, or manually out-of-service (unlocked/disabled/idle) then the alarm condition is not valid.\nIf communication to the service does not come back within several minutes (e.g. the cardConnectionLost alarm does not clear), it may be necessary to connect to the card's console-port to get the status of the service. Consult card specific documentation about the console commands to obtain the card service state.\nIf you are not successful in connecting to the console, this could be due to either a networking problem, or a fault in the card. If the card is inaccessible via console, it can be recovered via the reset button, or by power cycling. Continued trouble may mean the card is having some hardware difficulty; please contact your Nokia support representative to determine the next step(s).\nTry to ping the internal fixed service ip address of the service member from the host which is running the active CNFG service. If pinging the service member from the CNFG host succeeds, then go to Step 4; else go to Step 5.\nDetermine if REM has a connection to the service member via the use of the netstat command on the host which has the active CNFG service The following command will give a list of IP addresses that REM has connected to via well-known port 20000:\nnetstat -a | grep 20000\nLook for an 'Established' connection to the service's IP address in the output of the above command. If the service's IP address is not found in the output and this is the first time you have visited this step, then go to Step 6. If the service's IP address is not found in the output and this is the second time you have visited this step, then go to Step 7.\nCheck the IP connections from the host that has the active CNFG service member to the switches and the routers. Check the connection to the card. If connection problems are found, they must be fixed. One can also verify that the appropriate service IP addresses have been plumbed and the appropriate service image has been downloaded to the card.\nTry switching the CNFG service to its currently standby hot member via MI GUI.\nStop and start the CNFG service via the stopCNFG and startCNFG commands, respectively. This will stop the REM process and restart it, among others within the CNFG service. Once the CNFG service is active, the virtual cluster can be switched back. Note that error recovery and provisioning ability will be affected if the CNFG service is not operational.\nRestart/reload the service. This may be done via the MI GUI.		

Table 24-83 WmmLSS_cardError

Alarm	Attributes	Applicable major release
Name: WmmLSS_cardError (4200) Type: mmeAlarm Package: ltemme.WmmLSS_cardError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that a hardware diagnostic failure has been detected. Depending on the criticality of the checks, alarms with various severities are generated.		
Remedial action: For the Critical Alarm, the card should be taken OOS and replaced.\nFor the Major Alarm, the card should be taken OOS and rebooted to see if the alarm clears. If it does not clear or there are other reports from the card (such as Asserts) reporting problems, leave the card OOS and contact your Nokia support representative.\nFor the Minor Alarm, contact your Nokia support representative for the correction procedure.		

Table 24-84 WmmLSS_cdrFileStorageSpaceThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_cdrFileStorageSpaceThreshold (5388) Type: mmeAlarm Package: ltemme.WmmLSS_ cdrFileStorageSpaceThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: CDRs file storage space threshold reached		
Remedial action: Continue to the next action only if the system does not clear the alarm:\ntest the accessibility to the Charging Gateway (ping command);\ntrace the route to the Charging Gateway (traceroute command).\nIf the problem persists, contact your Nokia support representative.		

Table 24-85 WmmLSS_cdrStorageSpaceThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_cdrStorageSpaceThreshold (4405) Type: mmeAlarm Package: ltemme.WmmLSS_ cdrStorageSpaceThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: CDRs storage space threshold reached		
Remedial action: Continue to the next action only if the system does not clear the alarm:\ntest the accessibility to the Charging Gateway (ping command);\ntrace the route to the Charging Gateway (traceroute command).\nIf the problem persists, contact your Nokia support representative.		

Table 24-86 WmmLSS_cgfNotResponding

Alarm	Attributes	Applicable major release
Name: WmmLSS_cgfNotResponding (4406) Type: mmeAlarm Package: ltemme.WmmLSS_cgfNotResponding Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: SGSN/CGF interface: CGF not responding		
Remedial action: Continue to the next action only if the system does not clear the alarm:\ntest the accessibility to the Charging Gateway (ping command);\ntrace the route to the Charging Gateway (traceroute command);\nIf the problem persists, contact your Nokia support representative.		

Table 24-87 WmmLSS_cgfServiceNotSupported

Alarm	Attributes	Applicable major release
Name: WmmLSS_cgfServiceNotSupported (4407) Type: mmeAlarm Package: ltemme.WmmLSS_cgfServiceNotSupported Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-87 WmmLSS_cgfServiceNotSupported (continued)

Alarm	Attributes	Applicable major release
Description: The Charging Gateway is not able to process the CDRs transmitted by the SGSN		
Remedial action: Continue to the next action only if the system does not clear the alarm:\n If the problem persists, contact your Nokia support representative.		

Table 24-88 WmmLSS_cgfSystemFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_cgfSystemFailure (4408) Type: mmeAlarm Package: ltemme.WmmLSS_cgfSystemFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: SGSN/CGF interface: 'system failure' response		
Remedial action: Continue to the next action only if the system does not clear the alarm:\nIf the problem persists, contact your Nokia support representative.		

Table 24-89 WmmLSS_cgfVersionNotSupported

Alarm	Attributes	Applicable major release
Name: WmmLSS_cgfVersionNotSupported (4409) Type: mmeAlarm Package: ltemme.WmmLSS_cgfVersionNotSupported Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The version of GTP' supported by the SGSN is not supported by the Charging Gateway.		
Remedial action: Continue to the next action only if the system does not clear the alarm:\ncheck GTP' version at Charging Gateway.\nIf the problem persists, contact your Nokia support representative.		

Table 24-90 WmmLSS_cmasFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_cmasFailure (4800) Type: mmeAlarm Package: ltemme.WmmLSS_cmasFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that there is software failure in s1mme or sbc modules, related to CMAS.		
Remedial action: Contact your Nokia support representative.		

Table 24-91 WmmLSS_cmasReceiveFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_cmasReceiveFailure (4801) Type: mmeAlarm Package: ltemme.WmmLSS_cmasReceiveFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that MME failed to receive an acknowledgement to a CMAS message.		
Remedial action: Verify that the S1mme links are up.\nAlarm can only be cleared manually by running 'alarm_cli --clear alarmName="LSS_cmasReceiveFailure' from the active MI.\nIf condition persists, contact your Nokia support representative."		

Table 24-92 WmmLSS_cmasSendFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_cmasSendFailure (4802) Type: mmeAlarm Package: ltemme.WmmLSS_cmasSendFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that there is a failure in sending a CMAS message over s1mme or sbc interfaces.		

Table 24-92 WmmLSS_cmasSendFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify that the S1mme and sbc links are up.\nAlarm can only be cleared manually by running 'alarm_cli --clear alarmName="LSS_cmasSendFailure' from the active MI.\nIf condition persists, contact your Nokia support representative."		

Table 24-93 WmmLSS_connectionLostToLDPpeer

Alarm	Attributes	Applicable major release
Name: WmmLSS_connectionLostToLDPpeer (5151) Type: mmeAlarm Package: ltemme.WmmLSS_connectionLostToLDPpeer Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: There is no LDP session with a peer (SDP far-end).		
Remedial action: Check configuration: SDP administrative state, SDP far-end IP address. Check IP connectivity between SAF and LDP peer IP address.\nManually clear the alarm.		

Table 24-94 WmmLSS_cpiAlrmCritical

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAlrmCritical (4201) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAlrmCritical Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAlrmCritical indicates the value of the VS.alrmCritical measurement monitored by the Critical Alarms Count CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Using the Maintenance Interface, examine the set of critical alarms or any other alarms recently raised and address them.\nThis alarm will clear automatically if the rate of critical alarm generation drops below the threshold.		

Table 24-95 WmmLSS_cpiAlrmMajor

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAlrmMajor (4202) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAlrmMajor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAlrmMajor indicates the value of the VS.alrmMajor measurement monitored by the Major Alarms Count CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Using the Maintenance Interface, examine the set of major alarms or any other alarms recently raised and address them.\nThis alarm will clear automatically if the rate of major alarm generation drops below the threshold.		

Table 24-96 WmmLSS_cpiAlrmMinor

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAlrmMinor (4203) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAlrmMinor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAlrmMinor indicates the value of the VS.alrmMinor measurement monitored by the Minor Alarms Count CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Using the Maintenance Interface, examine the set of minor alarms or any other alarms recently raised and address them.\nThis alarm will clear automatically if the rate of minor alarm generation drops below the threshold.		

Table 24-97 WmmLSS_cpiAlrmWarning

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAlrmWarning (4204) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAlrmWarning Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-97 WmmLSS_cpiAlrmWarning (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiAlrmWarning indicates the value of the VS.alrmWarning measurement monitored by the Warning Alarms Count CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Using the Maintenance Interface, examine the set of warning alarms or any other alarms recently raised and address them.\nThis alarm will clear automatically if the rate of warning alarm generation drops below the threshold.		

Table 24-98 WmmLSS_cpiAsrtEsc

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAsrtEsc (4205) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAsrtEsc Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAsrtEsc indicates the value of the VS.asrtESC measurement monitored by the Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: This alarm will clear automatically if the rate of escalating assert generation drops below the threshold. An automatic escalation would result in a switch over and should also drop the rate of assert generation.\nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service and a switch over has not occurred, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-99 WmmLSS_cpiAsrtNonEsc

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAsrtNonEsc (4206) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAsrtNonEsc Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAsrtNonEsc indicates the value of the VS.asrtNonESC measurement monitored by the Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.		

Table 24-99 WmmLSS_cpiAsrtNonEsc (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.\ nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-100 WmmLSS_cpiAsrtNonEscCritical

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAsrtNonEscCritical (4207) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAsrtNonEscCritical Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAsrtNonEscCritical indicates the value of the VS.asrtNonESCCritical measurement monitored by the Critical Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.\ nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-101 WmmLSS_cpiAsrtNonEscMajor

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAsrtNonEscMajor (4208) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAsrtNonEscMajor Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-101 WmmLSS_cpiAsrtNonEscMajor (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiAsrtNonEscMajor indicates the value of the VS.asrtNonESCMajor measurement monitored by the Major Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.\ nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-102 WmmLSS_cpiAsrtNonEscMinor

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAsrtNonEscMinor (4209) Type: mmeAlarm Package: Itemme.WmmLSS_cpiAsrtNonEscMinor Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAsrtNonEscMinor indicates the value of the VS.asrtNonESCMinor measurement monitored by the Minor Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.\ nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-103 WmmLSS_cpiAudErrCount

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAudErrCount (4210) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAudErrCount Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAudErrCount indicates the value of the VS.audErrCount measurement monitored by the Audit Errors CPI exceeded a threshold in the last 15 minute interval. Audits run at low priority to recover lost or stuck resources. Audits generate error reports describing any problems they find. The VS.audErrCnt measurement reports the number of individual errors found by audits during the interval.		
Remedial action: Although audits take recovery for each error they find, use the Maintenance Interface to examine the set of audit errors reported. If this alarm recurs or is ongoing due to the same set of audits, contact your Nokia support representative. If this alarm is new and coincides with the introduction of a software update, contact your Nokia support representative immediately.\nThis alarm will clear automatically if the rate of audit detected errors drops below the threshold.		

Table 24-104 WmmLSS_cpiAudManAct

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAudManAct (4211) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAudManAct Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiAudManAct, indicates the value of the VS.audManAct measurement monitored by the Audit Errors Requiring Manual Action CPI exceeded a threshold in the last 15 minute interval. Audits run at low priority to recover lost or stuck resources. Audits generate error reports describing any problems they find.. The VS.audManAct measurement reports the number of individual errors found by audits during the interval that require manual action for recovery.		
Remedial action: Using the Maintenance Interface, examine the set of audit errors reported and address them. Audit error reports requiring manual action should specify the actions needed to perform recovery. If this alarm is new and coincides with the introduction of a software update, contact your Nokia support representative immediately.\nThis alarm will clear automatically if the rate of audit detected errors requiring manual action drops below the threshold. However, this will not happen until the required manual recovery steps have been taken.		

Table 24-105 WmmLSS_cpiAudNewEvent

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiAudNewEvent (4212) Type: mmeAlarm Package: ltemme.WmmLSS_cpiAudNewEvent Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiAudNewEvent indicates the value of the VS.audNewEvent measurement monitored by the Audit Initiated Events CPI exceeded a threshold in the last 15 minute interval. Audits run at low priority to recover lost or stuck resources. Audits generate error reports describing any problems they find..The VS.audNewEvent measurement reports the number of times during the interval that an audit that ran without being part of an escalated recovery and found at least one error.		
Remedial action: Although audits take recovery for each error they find, use the Maintenance Interface to examine the set of audit errors reported. If this alarm recurs or is ongoing due to the same set of audits, contact your Nokia support representative. If this alarm is new and coincides with the introduction of a software update, contact your Nokia support representative immediately.\nThis alarm will clear automatically if the rate of audit invocations that detect errors drops below the threshold.		

Table 24-106 WmmLSS_cpiDropMGAllocConnReq

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiDropMGAllocConnReq (10264) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiDropMGAllocConnReq Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiDropMGAllocConnReq, indicates the value of the switch health count measurement, monitored when the number of allocated connection requests drops. CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Check media gateway logs for errors.		

Table 24-107 WmmLSS_cpiExceptionService

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiExceptionService (4213) Type: mmeAlarm Package: ltemme.WmmLSS_cpiExceptionService Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-107 WmmLSS_cpiExceptionService (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiExceptionService indicates the value of the VS.exceptionService measurement monitored by the Service Exceptions CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: The value of the VS.exceptionService measurement monitored by the Service Exceptions CPI exceeded a threshold in the last 15 minute interval. This alarm will clear automatically if the rate of exceptions drops below the threshold.\nDetermine if any other alarms have been recently raised on the resource reported and address them.\nExamine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the PM counts indicates degradation of service and a switch-over has not already occurred, switch the service to its redundant mate.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.\nIf the situation persists after two or more switch-overs of the pair within the service, then attempt to duplex fail the service.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-108 WmmLSS_cpiFileSysUsage

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiFileSysUsage (4214) Type: mmeAlarm Package: ltemme.WmmLSS_cpiFileSysUsage Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiFileSysUsage indicates the value of resource usage count VS.fileSysUsage monitored by the File System Usage CPI exceeded a threshold in the last 5-minute interval.		
Remedial action: Remove outdated and obsolete files to free the file system space.\nMove the important data files to other disks to free the file system space.\nWhen CPI alarm LSS_cpiFileSysUsage is fired for CDR host, don't remove CDR record files (under /app1/data0/cdrdata) and PCMD record files (under /app1/data0/pcmddata). Furthermore, double check timestamp of CDR records files under /app1/data0/cdrdata/app2/charging/stream1/primary. If many files are older than two PULL/PUSH intervals, then there might be CDR records file transfer issue, which should be fixed firstly. For non-CDR record or non-PCMD record files, follow step 1 or step 2.		

Table 24-109 WmmLSS_cpiGTPcResponseTOGn

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiGTPcResponseTOGn (4215) Type: mmeAlarm Package: ltemme.WmmLSS_cpiGTPcResponseTOGn Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiGTPcResponseTOGn, indicates that the value of VS.cpiGTPcResponseTOGn has exceeded a threshold in the last 15 minute interval. This counter monitors the percentage of GTP Requests sent over a Gn interface for which no Response is received by the MME. The Gn interface connects the MME with one or more SGSNs. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring SGSNs for error conditions or ongoing problems. Verify network connectivity and proper configuration between MME and SGSNs. If SGSNs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-110 WmmLSS_cpiGTPcResponseTOS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiGTPcResponseTOS3 (4216) Type: mmeAlarm Package: ltemme.WmmLSS_cpiGTPcResponseTOS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiGTPcResponseTOS3, indicates meeting a threshold of GTP response failure rate in the last 5 minute interval. This failure rate monitors the percentage of GTP Requests sent over an S3 interface for which no Response is received by the MME. The S3 interface connects the MME with one or more SGSNs. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring SGSNs for error conditions or ongoing problems. Verify network connectivity and proper configuration between MME and SGSNs. If SGSNs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the S3 interface have been reported. Contact your Nokia support representative.		

Table 24-111 WmmLSS_cpiGTPcResponseTOSv

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiGTPcResponseTOSv (4217) Type: mmeAlarm Package: ltemme.WmmLSS_cpiGTPcResponseTOSv Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiGTPcResponseTOSv indicates meeting a threshold of the GTPc Response Time out over Sv CPI (requests sent over an Sv interface for which no response is received).		
Remedial action: Check neighboring LVI(s) for error conditions or ongoing problems. Verify network connectivity and proper configuration between MME and LVI(s). If LVI(s) and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-112 WmmLSS_cpiHOfailuresFrom2g3goverGn

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresFrom2g3goverGn (8028) Type: mmeAlarm Package: ltemme.WmmLSS_cpiHOfailuresFrom2g3goverGn Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresFrom2g3goverGn, indicates that the value of (100 - (100 * (VS. NbrHOtoLTESuccessGn / VS.AttNbrHOtoLTEGn)) has has exceeded a threshold in the last 5 minute interval. This value monitors the percentage of failure rate of attempted handovers from GERAN/UTRAN to MME using the Gn interface. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the Gn link status and MME service status.\nCheck fs.log for error indications related to Gn interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-113 WmmLSS_cpiHOfailuresFromGERANoverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresFromGERANoverS3 (4219) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresFromGERANoverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresFromGERANoverS3, indicates that the value of VS. cpiHOfailuresFromGERANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from GERAN to a E-UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-114 WmmLSS_cpiHOfailuresFromUTRANoverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresFromUTRANoverS3 (4220) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresFromUTRANoverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresFromUTRANoverS3, indicates that the value of VS. cpiHOfailuresFromUTRANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from UTRAN to a E-UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-115 WmmLSS_cpiHOfailuresRAUto2G3GnewSgwOverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiHOfailuresRAUto2G3GnewSgwOverS3 (4222) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresRAUto2G3GnewSgwOverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GnewSgwOverS3, indicates that the value of VS. cpiHOfailuresRAUto2G3GnewSgwOverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted RAU-based handovers from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface with SGW Relocation. This is Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-116 WmmLSS_cpiHOfailuresRAUto2G3GOverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresRAUto2G3GOverS3 (4221) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresRAUto2G3GOverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GOverS3, indicates the failure rate of attempted Routing Area Update (RAU) procedures from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface has exceeded a threshold in the last 5 minute interval. Failures encountered during the entire duration of the RAU procedure are included. Therefore, failures encountered both prior to and after SGW change determination are included. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-117 WmmLSS_cpiHOfailuresRAUto2G3GsameSgwOverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiHOfailuresRAUto2G3GsameSgwOverS3 (4223) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresRAUto2G3GsameSgwOverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GsameSgwOverS3, indicates that the value of VS. cpiHOfailuresRAUto2G3GsameSgwOverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface without SGW Relocation. This is Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-118 WmmLSS_cpiHOFailuresTo3G2GOverGn

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOFailuresTo3G2GOverGn (4218) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOFailuresTo3G2GOverGn Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOFailuresTo3G2GOverGn, indicates that the value of VS.cpiHOFailuresto3G2GOverGn has exceeded a threshold in the last 15 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN/GERAN SGSN using the Gn interface. This includes Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the Gn link status and MME service status.\nCheck fs.log for error indications related to Gn interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-119 WmmLSS_cpiHOfailuresToGERANoverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresToGERANoverS3 (4224) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresToGERANoverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresToGERANoverS3, indicates that the value of VS.cpiHOfailuresToGERANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a GERAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-120 WmmLSS_cpiHOfailuresToUTRANoverS3

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiHOfailuresToUTRANoverS3 (4225) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiHOfailuresToUTRANoverS3 Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiHOfailuresToUTRANoverS3, indicates that the value of VS.cpiHOfailuresToUTRANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.\nFor failures attributed to the MME, check the S3 link status and MME service status.\nCheck fs.log for error indications related to S3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-121 WmmLSS_cpiInterSgsn2GrauFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiInterSgsn2GrauFailures (8029) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiInterSgsn2GrauFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiInterSgsn2GrauFailures, indicates that the 2G value of VS.Gmm_succInterSgsnRaUpdate has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed Inter SGSN RAU Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Verify network connectivity and proper configuration between WMMs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-122 WmmLSS_cpiInterSgsn3GrauFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiInterSgsn3GrauFailures (8030) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiInterSgsn3GrauFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiInterSgsn3GrauFailures, indicates that the 3G value of VS.Gmm_succInterSgsnRaUpdate has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed Inter SGSN RAU Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Verify network connectivity and proper configuration between WMMs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-123 WmmLSS_cpiInterSgsnSrnsFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiInterSgsnSrnsFailures (8031) Type: mmeAlarm Package: ltemme.WmmLSS_cpiInterSgsnSrnsFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiInterSgsnSrnsFailures, indicates that the value of VS.Gmm_succInterSgsnRelocation_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed Inter SGSN SRNS Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Verify network connectivity and proper configuration between WMMs and SGSNs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-124 WmmLSS_cpiIntraSgsn2GrauFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiIntraSgsn2GrauFailures (8032) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiIntraSgsn2GrauFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiIntraSgsn2GrauFailures, indicates that the 2G value of VS.Gmm_succIntraSgsnRaUpdate has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN RAU Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-125 WmmLSS_cpiIntraSgsn3GrauFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiIntraSgsn3GrauFailures (8033) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiIntraSgsn3GrauFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiIntraSgsn3GrauFailures, indicates that the 3G value of VS.Gmm_succIntraSgsnRaUpdate has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN RAU Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-126 WmmLSS_cpiIntraSgsnSrnsFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiIntraSgsnSrnsFailures (8034) Type: mmeAlarm Package: ltemme.WmmLSS_cpiIntraSgsnSrnsFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiIntraSgsnSrnsFailures, indicates that the value of VS.Gmm_succIntraSgsnRelocation_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed Intra SGSN SRNS Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check WMM for internal error conditions or ongoing problems. Examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-127 WmmLSS_cpiMafAttachFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafAttachFailuresSysRelated (4233) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafAttachFailuresSysRelated Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafAttachFailuresSysRelated, indicates meeting/exceeding a threshold of the rate of system-related failures for Attach procedures, which is calculated every 5 minutes.		
Remedial action: Verify that the S1, S6a and S11 links are in-service/normal, using the link_cli command.\nVerify that no overload alarms exist on the MME.\nContact your Nokia support representative		

Table 24-128 WmmLSS_cpiMafAttachWithPGWreselection

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafAttachWithPGWreselection (4803) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafAttachWithPGWreselection Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm cpiAttachWithPGWreselection indicates meeting a threshold of the rate of PGW reselection during Attach procedures CPI.		
Remedial action: Contact your Nokia support representative.		

Table 24-129 WmmLSS_cpiMafAttachWithSGWreselection

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafAttachWithSGWreselection (4804) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafAttachWithSGWreselection Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-129 WmmLSS_cpiMafAttachWithSGWreselection (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm cpiAttachWithSGWreselection indicates meeting a threshold of the rate of SGW reselection during Attach procedures CPI.		
Remedial action: Contact your Nokia support representative.		

Table 24-130 WmmLSS_cpiMAFCommunicationFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMAFCommunicationFailureRate (4226) Type: mmeAlarm Package: Itemme.WmmLSS_ cpiMAFCommunicationFailureRate Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0
Description: The raised alarm, cpiMAFCommunicationFailureRate, indicates meeting a threshold of MAF communication failure rate on a per MAF service basis in the last 5 minutes. The failure rate is calculated from the measurement count VS.TotalMsgsRcvdFromMAF and VS.TotalMsgsSentToMAF in every interval of 5 minutes. On the MI GUI the alarm resource will indicate which MAF service has the problem in the MAF pool.		
Remedial action: Check the overload status of the MAF service firing this alarm.\nCheck if there is any hung process in the MAF service firing this alarm.\nIf the MAF service is duplex, try to switch the active MAF service.\nContact your Nokia support representative if problem still persists.		

Table 24-131 WmmLSS_cpiMafEIRfailuresS13

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafEIRfailuresS13 (4234) Type: mmeAlarm Package: Itemme.WmmLSS_cpiMafEIRfailuresS13 Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafEIRfailuresS13, indicates that the value of VS.LSS_cpiMafEIRfailuresS13 has exceeded a threshold in the last 5 minute interval. This counter monitors the percentage of unsuccessful EquipmentCheckRequest (ECR) to the number of ECRs attempted. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify the far end HSS (EIR) is functioning properly. Check fs.log for any ECR/ECA/S13 related errors to aid in determining the cause. Contact your Nokia support representative.		

Table 24-132 WmmLSS_cpiMafExtServiceReqFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMafExtServiceReqFailuresSysRelated (4235) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafExtServiceReqFailuresSysRelated Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMafExtServiceReqFailuresSysRelated indicates meeting a threshold of the Extended Service Request System Related Failure CPI.		
Remedial action: Verify that S1, S6a, S11 and SGs links are Unlocked/Enabled using link_cli\nVerify that there are no overload alarms on MME\nContact Your Nokia support representative		

Table 24-133 WmmLSS_cpiMafExtServiceRequestFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafExtServiceRequestFailures (4236) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafExtServiceRequestFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMafExtServiceRequestFailures indicates meeting a threshold of the Extended Service Request Failure CPI.		
Remedial action: Verify MME provisioning data, especially PLMN, TAI-LAI-Mapping, LAI tables\nVerify that S1, S6a, S11 and SGs links are Unlocked/Enabled using link_cli\nVerify that there are no overload alarms on MME\nContact your Nokia support representative		

Table 24-134 WmmLSS_cpiMafFailuresOverSGs

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafFailuresOverSGs (4237) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafFailuresOverSGs Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-134 WmmLSS_cpiMafFailuresOverSGs (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiMafFailuresOverSGs, indicates meeting/exceeding a threshold of the rate of failure for handling messages from the SGs interface, which is calculated every 5 minutes.		
Remedial action: Verify that the SGs links are in-service/normal, using the link_cli command.\nContact your Nokia support representative		

Table 24-135 WmmLSS_cpiMafHLRAuthFail

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafHLRAuthFail (4238) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafHLRAuthFail Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafHLRAuthFail, indicates meeting/exceeding a threshold of the rate of failure for handling Authentication failure messages from the HLR, which is calculated every 5 minutes.		
Remedial action: Verify that the Gr link is in-service/normal, using the link_cli command.\nContact your Nokia support representative		

Table 24-136 WmmLSS_cpiMafHSSreselection

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafHSSreselection (4805) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMafHSSreselection Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm cpiHSSreselection indicates meeting a threshold of the rate of HSS reselection during Authentication or Update Location procedures CPI.		
Remedial action: Contact your Nokia support representative.		

Table 24-137 WmmLSS_cpiMafPDNconnWithPGWreselection

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMafPDNconnWithPGWreselection (4806) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafPDNconnWithPGWreselection Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm cpiPDNconnWithPGWreselection indicates meeting a threshold of the rate of PGW reselection during PDN connectivity procedures CPI.		
Remedial action: Contact your Nokia support representative.		

Table 24-138 WmmLSS_cpiMafServiceReqFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMafServiceReqFailuresSysRelated (4239) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafServiceReqFailuresSysRelated Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafServiceReqFailuresSysRelated, indicates meeting/exceeding a threshold of the rate of system-related failures for UE Service Request procedures, which is calculated every 5 minutes.		
Remedial action: Verify that the S1, S6a and S11 links are in-service/normal, using the link_cli command.\nVerify that no overload alarms exist on the MME.\nContact your Nokia support representative		

Table 24-139 WmmLSS_cpiMafTauFailuresInterMme

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafTauFailuresInterMme (4240) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafTauFailuresInterMme Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-139 WmmLSS_cpiMafTauFailuresInterMme (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiMafTauFailuresInterMme, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving MME relocation which is calculated every 5 minutes.		
Remedial action: Verify that the eNB, and MME links are in-service/normal, using the link_cli command.\nContact your Nokia support representative to determine the status of the serving eNB and the MME groups serving the eNB that is involved in the TAU procedure		

Table 24-140 WmmLSS_cpiMafTauFailuresInterMmeInterSgw

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMafTauFailuresInterMmeInterSgw (4241) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafTauFailuresInterMmeInterSgw Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafTauFailuresInterMmeInterSgw, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving MME relocation and SGW relocation which is calculated every 5 minutes.		
Remedial action: Verify that the HSS, eNB, SGW, and MME links are in-service/normal, using link_cli.\nVerify UE subscription information in HSS.\nContact your Nokia support representative to determine the status of the serving eNB, MME groups, and SGW Pools serving the eNB that are involved in the TAU procedure.		

Table 24-141 WmmLSS_cpiMafTauFailuresInterSgw

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMafTauFailuresInterSgw (4242) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMafTauFailuresInterSgw Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMafTauFailuresInterSgw, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving SGW relocation, which is calculated every 5 minutes.		
Remedial action: Verify that the eNB, and SGW links are in-service/normal, using the link_cli command.\nContact your Nokia support representative to determine the status of the serving eNB and the SGW Pools serving the eNB that is involved in the TAU procedure		

Table 24-142 WmmLSS_cpiMBMSSessionStartM3FailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionStartM3FailureRate (4227) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionStartM3FailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionStartM3FailureRate indicates meeting a threshold of the MBMS Session Start M3 Failure Rate CPI.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.\nFor failures attributed to the MME, check the M3 link status and MME service status.\nCheck fs.log for error indications related to M3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-143 WmmLSS_cpiMBMSSessionStartSmFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionStartSmFailureRate (4228) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionStartSmFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionStartSmFailureRate indicates meeting a threshold of the MBMS Session Start Sm Failure Rate CPI.		
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.\nFor failures attributed to the MME, check the Sm link status and MME service status.\nCheck fs.log for error indications related to Sm interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-144 WmmLSS_cpiMBMSSessionStopM3FailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionStopM3FailureRate (4229) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionStopM3FailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionStopM3FailureRate indicates meeting a threshold of the MBMS Session Stop M3 Failure Rate CPI.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.\nFor failures attributed to the MME, check the M3 link status and MME service status.\nCheck fs.log for error indications related to M3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-145 WmmLSS_cpiMBMSSessionStopSmFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionStopSmFailureRate (4230) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionStopSmFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionStopSmFailureRate indicates meeting a threshold of the MBMS Session Stop Sm Failure Rate CPI.		
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.\nFor failures attributed to the MME, check the Sm link status and MME service status.\nCheck fs.log for error indications related to Sm interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-146 WmmLSS_cpiMBMSSessionUpdateM3FailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionUpdateM3FailureRate (4231) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionUpdateM3FailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionUpdateM3FailureRate indicates meeting a threshold of the MBMS Session Update M3 Failure Rate CPI.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.\nFor failures attributed to the MME, check the M3 link status and MME service status.\nCheck fs.log for error indications related to M3 interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-147 WmmLSS_cpiMBMSSessionUpdateSmFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiMBMSSessionUpdateSmFailureRate (4232) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiMBMSSessionUpdateSmFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiMBMSSessionUpdateSmFailureRate indicates meeting a threshold of the MBMS Session Update Sm Failure Rate CPI.		
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.\nFor failures attributed to the MME, check the Sm link status and MME service status.\nCheck fs.log for error indications related to Sm interface procedures, contact your Nokia support representative if internal MME errors are indicated.		

Table 24-148 WmmLSS_cpiMemAllocFail

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiMemAllocFail (4243) Type: mmeAlarm Package: ltemme.WmmLSS_cpiMemAllocFail Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiMemAllocFail, indicates the value of the VS.memAllocFail measurement monitored by the failed memory allocation attempts CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: Investigate the amount of load being handled by this service and take steps to reduce it if it is excessive. Otherwise contact your Nokia support representative. If this alarm coincides with the introduction of a software update, contact your Nokia support representative immediately.\nThis alarm will clear automatically if the rate of memory allocation failures drops below the threshold.		

Table 24-149 WmmLSS_cpiNoPSHOFailuresOverSv

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiNoPSHOFailuresOverSv (4244) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiNoPSHOFailuresOverSv Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiNoPSHOFailuresOverSv indicates meeting a threshold of the Hand Down to UTRAN/GERAN via the Sv interface without PSHO Failure Rate CPI.		
Remedial action: Check counters and alarms related to the Sv interface. Verify network connectivity and proper configuration between the MME and LVI(s).\nCheck the target UTRAN/GERAN network for configuration problems that could cause the handover preparation attempts to be rejected.\nCheck the source E-UTRAN network and target UTRAN/GERAN network for handover failure conditions.\nCheck fs.log for error indications related to Sv interface procedures. Contact your Nokia support representative if internal MME errors are indicated.		

Table 24-150 WmmLSS_cpiPSHOFailuresOverSv

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiPSHOFailuresOverSv (4245) Type: mmeAlarm Package: ltemme.WmmLSS_cpiPSHOFailuresOverSv Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiPSHOFailuresOverSv indicates meeting a threshold of the Hand Down to UTRAN/GERAN via the Sv interface with PSHO Failure Rate CPI.		
Remedial action: Check counters and alarms related to the Sv interface. Verify network connectivity and proper configuration between the MME and MSC(s).\nCheck the target UTRAN/GERAN network for configuration problems that could cause the handover preparation attempts to be rejected.\nCheck the source E-UTRAN network and target UTRAN/GERAN network for handover failure conditions.\nCheck fs.log for error indications related to Sv interface procedures. Contact your Nokia support representative if internal MME errors are indicated.		

Table 24-151 WmmLSS_cpiReinitServiceSelf

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiReinitServiceSelf (4246) Type: mmeAlarm Package: ltemme.WmmLSS_cpiReinitServiceSelf Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiReinitServiceSelf indicates the value of the VS.reinitServiceSelf measurement monitored by the Automatic Service Re-initialization CPI exceeded a threshold in the last 15 minute interval.		
Remedial action: This alarm will clear automatically if the rate of re-initializations drops below the threshold.\nCheck that a switch over has successfully occurred.\nDetermine if any other alarms have been recently raised on the resource reported and address them. As this is likely the result of recovery escalation, one or more of these alarms may also be raised: LSS_cpiAsrtEsc, LSS_cpiExceptionService, LSS_cpiRestartTask\nIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.\nIf a Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact your Nokia support representative.\nIf the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service if that has not already occurred.\nIf the situation persists after two or more switch-overs of the pair within the service, then attempt to duplex fail the service.\nAttempt to power down the card providing the service and then restore it. If the problem clears, this suggests faulty hardware.\nIn all cases, contact your Nokia support representative regarding this alarm.		

Table 24-152 WmmLSS_cpiS3TauFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiS3TauFailures (4247) Type: mmeAlarm Package: ltemme.WmmLSS_cpiS3TauFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiS3TauFailures, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal, using link_cli.\nVerify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.\nVerify the operational status of the DNS server and that the DNS entries for the SGW are correct.\nContact your Nokia support representative to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 24-153 WmmLSS_cpiS3TauFailuresInterSgw

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiS3TauFailuresInterSgw (4248) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiS3TauFailuresInterSgw Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiS3TauFailuresInterSGW, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link that involves a change of serving SGW.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal, using link_cli.\nVerify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.\nVerify the operational status of the DNS server and that the DNS entries for the SGW are correct.\nContact your Nokia support representative to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 24-154 WmmLSS_cpiS3TauFailuresIntraSGW

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiS3TauFailuresIntraSGW (4249) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiS3TauFailuresIntraSGW Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiS3TauFailuresIntraSGW, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link that do not involve a change of serving SGW.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal, using link_cli.\nVerify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.\nVerify the operational status of the DNS server and that the DNS entries for the SGW are correct.\nContact your Nokia support representative to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 24-155 WmmLSS_cpiSgsn2GattachFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn2GattachFailures (8037) Type: mmeAlarm Package: ltemme.WmmLSS_cpiSgsn2GattachFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn2GattachFailures, indicates that the 2G value of VS.Gmm_succGprsAttach has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN Attach Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check EIR and/or HSS for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and EIR and/or HSS. Examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-156 WmmLSS_cpiSgsn2GpagingFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn2GpagingFailures (8038) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn2GpagingFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn2GpagingFailures, indicates that the 2G value of VS.Gmm_unsuccPacketSwitchingPaging has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN Paging Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check GERAN for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and GERAN. Contact your Nokia support representative.		

Table 24-157 WmmLSS_cpiSgsn2GpdpActivationFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn2GpdpActivationFailures (8039) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn2GpdpActivationFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn2GpdpActivationFailures, indicates that the 2G value of VS.Sm_ succActPDPCtxMSPerSgsn has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Activation. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring SGW and GGSN for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and SGW and GGSN. If WMM and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-158 WmmLSS_cpiSgsn2GpdpDeactNwFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn2GpdpDeactNwFailures (8040) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn2GpdpDeactNwFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn2GpdpDeactNwFailures, indicates that the 2G sum of VS.Sm_succGgsnDeactPDPCtx_G and VS.Sm_succSgsnDeactPDPCtx_G has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Deactivation NW. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring GERANs for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and GERANs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-159 WmmLSS_cpiSgsn3GattachFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn3GattachFailures (8041) Type: mmeAlarm Package: ltemme.WmmLSS_cpiSgsn3GattachFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn3GattachFailures, indicates that the 3G value of VS.Gmm_succGprsAttach has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN Attach Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check EIR and/or HSS for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and EIR and/or HSS. Examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-160 WmmLSS_cpiSgsn3GpagingFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn3GpagingFailures (8042) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn3GpagingFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn3GpagingFailures, indicates that the 3G value of VS.Gmm_unsuccPacketSwitchingPaging has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN Paging Procedure. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check UTRAN for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and UTRAN. Contact your Nokia support representative.		

Table 24-161 WmmLSS_cpiSgsn3GpdpActivationFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn3GpdpActivationFailures (8043) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn3GpdpActivationFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn3GpdpActivationFailures, indicates that the 3G value of VS.Sm_ succActPDPCtxMSPerSgsn has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Activation. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring SGW and GGSN for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and SGW and GGSN. If WMM and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-162 WmmLSS_cpiSgsn3GpdpDeactNwFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsn3GpdpDeactNwFailures (8044) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsn3GpdpDeactNwFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsn3GpdpDeactNwFailures, indicates that the 3G sum of VS.Sm_succGgsnDeactPDPCtx_U and VS.Sm_succSgsnDeactPDPCtx_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Deactivation NW. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring UTRANs for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and UTRANs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-163 WmmLSS_cpiSgsnPdpDeact2GmsFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsnPdpDeact2GmsFailures (8045) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsnPdpDeact2GmsFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsnPdpDeact2GmsFailures, indicates that the value of VS.Sm_succMSDeactPDPCtx_G has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Deactivation 2G MS. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring GGSN and SGW for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and GERANs. If WMM and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-164 WmmLSS_cpiSgsnPdpDeact3GmsFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsnPdpDeact3GmsFailures (8046) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsnPdpDeact3GmsFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsnPdpDeact3GmsFailures, indicates that the value of VS.Sm_succMSDeactPDPCtx_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Deactivation 3G MS. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring GGSN and SGW for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and UTRANs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-165 WmmLSS_cpiSgsnPdpMod3GmsFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsnPdpMod3GmsFailures (8047) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsnPdpMod3GmsFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsnPdpMod3GmsFailures, indicates that the value of VS.Sm_succModPDPCtxMs_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Modification 3G MS. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring GGSN and SGW for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM and UTRANs. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-166 WmmLSS_cpiSgsnPdpMod3GnwFailures

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSgsnPdpMod3GnwFailures (8048) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSgsnPdpMod3GnwFailures Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_cpiSgsnPdpMod3GnwFailures, indicates that the value of VS.Sm_succModPDPCtxSgsn_U has crossed a threshold in the last 15 minute interval. This counter monitors the percentage of failed SGSN PDP Context Modification 3G NW. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check neighboring UTRANs for error conditions or ongoing problems. Verify network connectivity and proper configuration between WMM, SGW and GGSN. If WMMs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact your Nokia support representative.		

Table 24-167 WmmLSS_cpiSS7DropSCTPPktsRcvd

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSS7DropSCTPPktsRcvd (8035) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiSS7DropSCTPPktsRcvd Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm, LSS_cpiSS7DropSCTPPktsRcvd, indicates the drop rate for transmitting SCTP packets (VS. SctpInSCTPPacks).		
Remedial action: Check to see if the IP network is experiencing congestion. If so, resolve the congestion and check if the alarm clear.\nIf the alarm is not cleared, there is possibly an inconsistency with the provisioned data for the SS7 connections. Verify the consistency of the provisioned data on the local system and the remote system.\nIf the alarm is not cleared, contact your Nokia support representative. It is possible that there is data corruption which may require deleting and re-growing the SS7 connections or initializing the SS7 card		

Table 24-168 WmmLSS_cpiSS7FailSCTPFastRetransRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiSS7FailSCTPFastRetransRate (8036) Type: mmeAlarm Package: ltemme.WmmLSS_cpiSS7FailSCTPFastRetransRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates the SCTP Fast Retransmit Count on a given card, is in a high percentage of the total outgoing SCTP packet count. The SCTP Fast Retransmit Rate CPI (Component Performance Indicator), is calculated every 5 minutes.		
Remedial action: Check to see if the IP network is experiencing congestion. If so, resolve the congestion and check if the alarm clear.\nIf the alarm is not cleared, contact your Nokia support representative.		

Table 24-169 WmmLSS_cpiStopWarnMsgDeliveryS1MMEFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiStopWarnMsgDeliveryS1MMEFailureRate (4250) Type: mmeAlarm Package: ltemme.WmmLSS_cpiStopWarnMsgDeliveryS1MMEFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiStopWarnMsgDeliveryS1MMEFailureRate indicates meeting a threshold of the Stop Warning Message Delivery S1MME Failure Rate CPI.		
Remedial action: Verify that the S1MME links are in-service/normal, using link_cli.\nVerify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.\nContact your Nokia support representative to determine the status of the eNBs that are involved in the Stop Warning Message procedure.		

Table 24-170 WmmLSS_cpiStopWarnMsgDeliverySBcFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiStopWarnMsgDeliverySBcFailureRate (4251) Type: mmeAlarm Package: ltemme.WmmLSS_cpiStopWarnMsgDeliverySBcFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-170 WmmLSS_cpiStopWarnMsgDeliverySBcFailureRate (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiStopWarnMsgDeliverySBcFailureRate indicates meeting a threshold of the Stop Warning Message Delivery SBc Failure Rate CPI.		
Remedial action: Verify that the SBC links are in-service/normal, using link_cli.\nVerify that the S1MME links are in-service/normal, using link_cli.\nVerify the operational status of the CBC.\nVerify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.\nContact your Nokia support representative to determine the status of the CBC and eNBs that are involved in the Stop Warning Message procedure.		

Table 24-171 WmmLSS_cpiUECapacityUsage

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpiUECapacityUsage (4252) Type: mmeAlarm Package: ltemme.WmmLSS_cpiUECapacityUsage Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, cpiUECapacityUsage, indicates meeting a threshold of a UE capacity utilization rate on a per MAF service basis in the last 5 minutes.		
Remedial action: Check how many MAF services the MME has and consider to install more MAF services to increase the MME capacity.		

Table 24-172 WmmLSS_cpiWarnMsgDeliveryS1MMEFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiWarnMsgDeliveryS1MMEFailureRate (4253) Type: mmeAlarm Package: ltemme.WmmLSS_ cpiWarnMsgDeliveryS1MMEFailureRate Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiWarnMsgDeliveryS1MMEFailureRate indicates meeting a threshold of the Warning Message Delivery S1MME Failure Rate CPI.		
Remedial action: Verify that the S1MME links are in-service/normal, using link_cli.\nVerify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.\nContact your Nokia support representative to determine the status of the eNBs that are involved in the Write Replace Warning Message procedure.		

Table 24-173 WmmLSS_cpiWarnMsgDeliverySBcFailureRate

Alarm	Attributes	Applicable major release
Name: WmmLSS_ cpiWarnMsgDeliverySBcFailureRate (4254) Type: mmeAlarm Package: Itemme.WmmLSS_ cpiWarnMsgDeliverySBcFailureRate Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_cpiWarnMsgDeliverySBcFailureRate indicates meeting a threshold of the Warning Message Delivery SBc Failure Rate CPI.		
Remedial action: Verify that the SBC links are in-service/normal, using link_cli.\nVerify that the S1MME links are in-service/normal, using link_cli.\nVerify the operational status of the CBC.\nVerify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.\nContact your Nokia support representative to determine the status of the CBC and eNBs that are involved in the Write Replace Warning Message procedure.		

Table 24-174 WmmLSS_cpuOverload

Alarm	Attributes	Applicable major release
Name: WmmLSS_cpuOverload (4255) Type: mmeAlarm Package: Itemme.WmmLSS_cpuOverload Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the CPU utilization on a service has exceeded the threshold. The overload could be caused by one or more of the following reasons: base overload, per-service quota restriction overload or thread level CPU overload. The 'Additional Info' field of the alarm report will list the contributing causes. When thread level CPU overload level changes, a corresponding profile report is also generated.		
Remedial action: Verify that no running debug or testing tool is running that uses a lot of CPU.\nIf CPU utilization regularly exceeds thresholds, investigate how the call traffic load can be reduced:\nReengineer so less traffic is directed to this office or card.\nIf your application supports higher-capacity cards, consider replacing them\nVerify if there are enough call servers, device servers, etc., to handle the expected load and add additional cards as appropriate.		

Table 24-175 WmmLSS_databaseConnectionLost

Alarm	Attributes	Applicable major release
Name: WmmLSS_databaseConnectionLost (4257) Type: mmeAlarm Package: ltemme.WmmLSS_databaseConnectionLost Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm can be displayed during the initiation of CNFG server (startFS or startCNFG), when the host_manager fails to connect to the database.		
Remedial action: Stop and restart the database using the following commands:\nstopFS\nsudo RCCmachoffine -u\nsudo RCCmachonline\nstartFS\nIf this alarm is fired from CDR host and not cleared, contact your Nokia support representative.		

Table 24-176 WmmLSS_databaseReplicationLinkDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_databaseReplicationLinkDown (4258) Type: mmeAlarm Package: ltemme.WmmLSS_databaseReplicationLinkDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when a database replication link is down.		
Remedial action: The host on one end of the bad link should be brought gracefully offline and online. Any active services on the blade should be switched to the mate host prior to bring the host offline. When the host is back online check replications links using 'lss login, type dbcli -R'.		

Table 24-177 WmmLSS_databaseSizeExhausted

Alarm	Attributes	Applicable major release
Name: WmmLSS_databaseSizeExhausted (4259) Type: mmeAlarm Package: ltemme.WmmLSS_databaseSizeExhausted Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-177 WmmLSS_databaseSizeExhausted (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when a database approaches full capacity.		
Remedial action: If the alarm is a warning (84% full), the system impact on the specified database reaching capacity should be investigated. In some instances, a database at 84% capacity is acceptable. Contact your Nokia support representative for additional details.\nIf the alarm becomes Major (96% full), field support should be contacted. In most cases, steps to reduce the size of the database should be implemented. Contact your Nokia support representative to assist in the investigation to reduce the size of the impacted database.		

Table 24-178 WmmLSS_dataMismatch

Alarm	Attributes	Applicable major release
Name: WmmLSS_dataMismatch (4256) Type: mmeAlarm Package: ltemme.WmmLSS_dataMismatch Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A data mismatch has been detected, which indicates that there has been an error in provisioning. The additionalText field of the event provides the details of the data mismatch.		
Remedial action: A data mismatch has been detected, which indicates that there has been an error in provisioning. The mismatch is most probably between the configurations of the SCTP profile and Interface profile and between the network interface types. Another probable cause is that provisioned for an interface do not match the IP addresses learned from the remote end in the SCTP INIT-ACK message. \nThis alarm must be manually cleared after the provisioned data is corrected.		

Table 24-179 WmmLSS_dbHighCpuUtilization

Alarm	Attributes	Applicable major release
Name: WmmLSS_dbHighCpuUtilization (4260) Type: mmeAlarm Package: ltemme.WmmLSS_dbHighCpuUtilization Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates very high CPU time usage by a database system process.		
Remedial action: The host and pid of the process are printed in the alarm. Monitor CPU usage of this pid and contact your Nokia support representative. This condition can generally be cleared by stopping and then starting RCC VM on the affected host.		

Table 24-180 WmmLSS_dbOffline

Alarm	Attributes	Applicable major release
Name: WmmLSS_dbOffline (4261) Type: mmeAlarm Package: ltemme.WmmLSS_dbOffline Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when the database is offline.		
Remedial action: Normally the alarm will be cleared automatically when Datablitz servers recover; If this alarm is not cleared, please contact your Nokia support representative.		

Table 24-181 WmmLSS_dbStatusUnexpected

Alarm	Attributes	Applicable major release
Name: WmmLSS_dbStatusUnexpected (4262) Type: mmeAlarm Package: ltemme.WmmLSS_dbStatusUnexpected Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when the DataBlitz database can not be accessed.		
Remedial action: Normally the alarm will be cleared automatically when Datablitz database(s) becomes accessible. If this alarm is not cleared, please contact your Nokia support representative.		

Table 24-182 WmmLSS_degradedResource

Alarm	Attributes	Applicable major release
Name: WmmLSS_degradedResource (4263) Type: mmeAlarm Package: ltemme.WmmLSS_degradedResource Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-182 WmmLSS_degradedResource (continued)

Alarm	Attributes	Applicable major release
Description: A Critical Application Resource (CAR) has reached a degraded condition that indicates some aspect of the switch is not performing as expected. The affected service member is indicated in the alarm by the PoolType, PoolId, and PoolMemberId.		
Remedial action: The root cause depends on the specific resource that is degraded.\nFrom the alarm, determine the service member that is degraded, as shown by the PoolType, PoolId, and PoolMemberId.\nOn the MI GUI, go to the Management Interface window. Under the appropriate shelf, click Service Members. In the Service Members window, right click the appropriate service member, and choose Display Degraded Critical Resources. A pop-up window will display the 'Resource name' for each resource that is causing the service member to be degraded.\nIn most cases, when a resource is degraded, the associated alarm will be firing.\nSee the entry for this alarm in the '9471 Mobility Management Entity Alarm Dictionary 418-111-208' for a list of resources and the associated alarms.		

Table 24-183 WmmLSS_degrow

Alarm	Attributes	Applicable major release
Name: WmmLSS_degrow (4264) Type: mmeAlarm Package: ltemme.WmmLSS_degrow Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM degrow procedure, failures that occur will result in the generation of DEGROW alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the DEGROW alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-184 WmmLSS_deviceServerCxnLost

Alarm	Attributes	Applicable major release
Name: WmmLSS_deviceServerCxnLost (5077) Type: mmeAlarm Package: ltemme.WmmLSS_deviceServerCxnLost Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm is generated when the mate-to-mate connection is lost for some service instance pairs. The service instance pairs that this alarm applies to includes: AMMS, H248, IMS, and the MPH.		
Remedial action: The alarm clears automatically when the switch-over is completed.\nIf the alarm is not the result of a manual action, then the alarm will automatically clear within a minute. Customer Technical Support should be contacted if the alarm does not clear automatically.\nIf the alarm is the result of a manual action, such as taking a host out of service, then the alarm will clear when the host is manually placed back into service.		

Table 24-185 WmmLSS_diskGoingDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_diskGoingDown (4265) Type: mmeAlarm Package: ltemme.WmmLSS_diskGoingDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the Smart Monitor Tool Set (smartmontools) has determined that the Disk Drive for this LCP Host is going down, and is predicting failure in the next 24 hours.		
Remedial action: Backup Recovery actions for this LCP Host should be immediately executed.\nContact your Nokia support representative immediately.		

Table 24-186 WmmLSS_diskMirrorFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_diskMirrorFailure (8394) Type: mmeAlarm Package: ltemme.WmmLSS_diskMirrorFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when Disk Mirroring Setup for 2G/3G Charging Records fails.		
Remedial action: Reboot the OAM blade hosting the safcha service. Once the reboot has completed, switch the active safcha service back onto this blade. If the alarm persists, contact your Nokia support representative.		

Table 24-187 WmmLSS_diskSector

Alarm	Attributes	Applicable major release
Name: WmmLSS_diskSector (4266) Type: mmeAlarm Package: ltemme.WmmLSS_diskSector Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the Smart Monitor Tool Set (smartmontools) has determined that the Disk Drive for this LCP Host has a bad sector.		

Table 24-187 WmmLSS_diskSector (continued)

Alarm	Attributes	Applicable major release
Remedial action: The card reporting the problem should be replaced, following the card replacement procedures.		

Table 24-188 WmmLSS_dnsThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_dnsThreshold (4267) Type: mmeAlarm Package: ltemme.WmmLSS_dnsThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates returned number of IP addresses in DNS query of diameter fully-qualified domain name (FQDN) exceeds its number threshold.		
Remedial action: Verify that destination FQDN is correctly provisioned on the GUI\nVerify that FQDN is correctly provisioned on the external DNS server(IP addresses count should be less than threshold value).		

Table 24-189 WmmLSS_ethernetError

Alarm	Attributes	Applicable major release
Name: WmmLSS_ethernetError (4268) Type: mmeAlarm Package: ltemme.WmmLSS_ethernetError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: One of the two Ethernet Links on a Service Host has failed.		
Remedial action: Regardless of the cause of the Ethernet Link alarm, integrity software running on the affected Service Host should automatically initiate a switch to redundant hardware to ensure that the effects of the failure are minimized. The following recovery actions may, in fact, be automatically initiated:\nService Host switch, if multiple Ethernet Links are affected\nEthernet Link switch, if a single Active Ethernet Link is affected\nNone, if the hardware failure affects a Standby Ethernet Link\nThe reason for the failure needs to be understood and corrected. It is possible that the Service Host Ethernet Port failed, the cabling that interconnects the Ethernet Port to the network is cut, the Routers and/or Ethernet Switches that make up the SoftSwitch Network failed. Investigate each of these reasons and discount or correct. Once corrected, the alarm will be cleared.		

Table 24-190 WmmLSS_ethernetLinkDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_ethernetLinkDown (4269) Type: mmeAlarm Package: ltemme.WmmLSS_ethernetLinkDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The redundant Ethernet link has gone down on one of the diskless hosts. A link switchover may have occurred to move communication for that host to the remaining link, which is now simplex.		
Remedial action: Determine if any related alarms are also present, such as on the ESC, chassis, or board itself. Correct those alarms first and see if this alarm clears as a result.\nOn CP 1000: Verify that the cable from the corresponding faceplate port to the external Ethernet router is connected and is good. Replace as necessary.\nOn other Nokia Products: Verify that the ESC corresponding to this link is operational by viewing its status at MI, and by telnet to the ESC card. Correct or replace ESC as necessary.\nOn 5400 LCP: Verify that the hub corresponding to this link is operational by viewing its status at MI, and by telnet to the Hub. Correct or replace Hub as necessary.\nOn CP 1000: Verify that the external Ethernet router is operational. Correct or replace as necessary.\nOn other Nokia Products: On the ESC verify that the Ethernet port corresponding to the card for this host is operational. Re-enable port as necessary.\nOn 5400 LCP: On the hub verify that the Ethernet port corresponding to the card for this host is operational. Re-enable port as necessary. Replace the card used for this host using the appropriate FRU procedure as necessary.\nOn CP 1000: Replace the card used for this host using the appropriate FRU procedure.\nIf the above steps do not clear the alarm, contact your Nokia support representative.		

Table 24-191 WmmLSS_excessiveExternalLinksDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_excessiveExternalLinksDown (4807) Type: mmeAlarm Package: ltemme.WmmLSS_excessiveExternalLinksDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: An excessive number of links of a given type (e.g. s1mme, s11, etc.) are down. This is usually due to a network connectivity problem and not the individual links between the WMM and the external entity. Once this alarm is triggered the WMM will stop reporting alarms and status for links of the given type. Once the network problem is resolved and the number of links down is no longer excessive, this alarm will clear and the status of all links of the given type will be updated. This alarm is raised when at least 100 links of a given type are down. This alarm clears when 95 or fewer links are down.		
Remedial action: Determine that there are no errors within the IP network.\nIf the network entity data is provisioned on MME, verify the data is correct.\nVerify the network entity that MME fails to communicate with is in service.		

Table 24-192 WmmLSS_externalConnectivity

Alarm	Attributes	Applicable major release
Name: WmmLSS_externalConnectivity (4270) Type: mmeAlarm Package: ltemme.WmmLSS_externalConnectivity Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The system detected a problem or a state change to external connectivity.		
Remedial action: For INFO alarm, there is no action needed.\nFor MAJOR and CRITICAL alarm, verify the cable connections from both HUB cards to customer layer 2 switches, check if the cables are plugged properly.\nFor MAJOR and CRITIAL alarm, verify the port status on HUB cards, the port connect to the customer network should be in service.\nFor MAJOR and CRITIAL alarm, verify the individual Ethernet port status on the HUB card for the given host with the alarm.\nFor the CRITIAL alarm, verify connectivity to/from each of the IPs listed in the ARP list from the given host with the alarm.\nCheck the next hop reported as failing.\nContact your Nokia support representative for the correction procedure if previous steps do not correct it.		

Table 24-193 WmmLSS_externalLinkConfigurationLimit

Alarm	Attributes	Applicable major release
Name: WmmLSS_externalLinkConfigurationLimit (4410) Type: mmeAlarm Package: ltemme.WmmLSS_externalLinkConfigurationLimit Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The maximum number of links for a given link type has been reached. When this limit is reached, it is not possible to create any new links of the given link type. Every 15 minutes a check will be performed in an attempt to recover any links which have not been used or have been disabled due to lack of far-end response. A configurable parameter, TdynMO , is used to control the aging algorithm for link recovery.		
Remedial action: Wait at least TdynMO time interval to allow the system to recover inactive or disabled links.\nIf the system does not recover any links after TdynMO time interval, contact your Nokia support representative.		

Table 24-194 WmmLSS_externalLinkDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_externalLinkDown (4271) Type: mmeAlarm Package: ltemme.WmmLSS_externalLinkDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Communication between WMM and another network entity can not be established.		
Remedial action: Verify the network entity that WMM fails to communicate with is in service.\nDetermine that there are no errors within the IP network.\nIf the network entity data is provisioned on WMM, verify the data is correct.\nIf multiple links that terminate on the MIF (X1_1 or X2) are down, try switching MIF to hot-standby mate.\nIf multiple links that terminate on the MPH (non-X1_1 and non-X2) are down, try switching MPH to hot-standby mate.		

Table 24-195 WmmLSS_failedAttachReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_failedAttachReqsRateExceeded (4272) Type: mmeAlarm Package: ltemme.WmmLSS_ failedAttachReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedAttachReqsRateExceeded, indicates the value of the VS.cpiAttachFailures measurement, monitored when failure Attach request CPI exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the UE Attach procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions		
Remedial action: Verify that the eNB, HSS and SGW links are in-service/normal, using the link_cli command.\nIf the links look normal, and the alarm persists, contact your Nokia support representative.		

Table 24-196 WmmLSS_failedAuthRequestsHSSRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedAuthRequestsHSSRateExceeded (4273) Type: mmeAlarm Package: ltemme.WmmLSS_ failedAuthRequestsHSSRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedAuthRequestsHSSRateExceeded, indicates the value of VS.cpiHSSauthFailures measurement, monitored when HSS failed Authentication requests exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Authentication procedure between the MME and the HSS, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions		
Remedial action: Clearance options include:\nEnsure communication between the MME and HSS (ping)\nIf the HSS (S6a) link looks normal (using the link_cli command), and alarm persists, contact your Nokia support representative.		

Table 24-197 WmmLSS_failedAuthRequestsUERateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedAuthRequestsUERateExceeded (4274) Type: mmeAlarm Package: ltemme.WmmLSS_ failedAuthRequestsUERateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedAuthRequestsUERateExceeded, indicates the value of VS.cpiUEauthFailures measurement, monitored when UE failed Authentication requests exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Authentication procedure between the MME and the UE and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify HSS and UE authentication data, using ueadmin_cli.\nIf the authentication data looks good, and the alarm persists, contact your Nokia support representative.		

Table 24-198 WmmLSS_failedCrDedBearerReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedCrDedBearerReqsRateExceeded (4275) Type: mmeAlarm Package: ltemme.WmmLSS_ failedCrDedBearerReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedCrDedBearerReqsRateExceeded, indicates the value of VS. cpiCreateDedicatedBearerFailures measurement, monitored when failure on Create Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Create Dedicated Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Contact your Nokia support representative.		

Table 24-199 WmmLSS_failedDeactDedBearerReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedDeactDedBearerReqsRateExceeded (4276) Type: mmeAlarm Package: ltemme.WmmLSS_ failedDeactDedBearerReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedDeactDedBearerReqsRateExceeded, indicates the value of VS. cpiDeactivateDedBearerFailures measurement, monitored when failure on Deactivate Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Deactivate Dedicated Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Contact your Nokia support representative.		

Table 24-200 WmmLSS_failedHRPDhandoverRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_failedHRPDhandoverRateExceeded (4277) Type: mmeAlarm Package: ltemme.WmmLSS_ failedHRPDhandoverRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedHRPDhandoverRateExceeded, indicates the value of VS.cpiHRPDHoFailures measurement, monitored when failure on a HRPD Handover request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Handover to HRPD procedure , and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Look at all the failure counters for the Handover to HRPD procedure in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 24-201 WmmLSS_failedMobileTermLocRequestRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedMobileTermLocRequestRateExceeded (4278) Type: mmeAlarm Package: ltemme.WmmLSS_ failedMobileTermLocRequestRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_failedMobileTermLocRequestRateExceeded indicates meeting a threshold of the Mobile Termination Location Request Failure CPI.		
Remedial action: Verify that the S1-MME and SLs links are in-service/normal, using link_cli.\nRefer to the Location Based Services failure counters to get a more specific failure reason.\nContact your Nokia support representative to determine the status of the SMLC that are involved in the LCS procedure.		

Table 24-202 WmmLSS_failedNetwrkInducedLocRequestRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedNetwrkInducedLocRequestRateExceeded (4279) Type: mmeAlarm Package: ltemme.WmmLSS_ failedNetwrkInducedLocRequestRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_failedNetwrkInducedLocRequestRateExceeded indicates meeting a threshold of the Network Induced Location Request Failure CPI.		
Remedial action: Verify that the S1-MME and SLs links are in-service/normal, using link_cli.\nRefer to the Location Based Services failure counters to get a more specific failure reason.\nContact your Nokia support representative to determine the status of the SMLC that are involved in the LCS procedure.		

Table 24-203 WmmLSS_failedNumHOFwdRelocRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedNumHOFwdRelocRateExceeded (4280) Type: mmeAlarm Package: ltemme.WmmLSS_ failedNumHOFwdRelocRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedNumHOFwdRelocRateExceeded, indicates the value of VS.cpiHOwMMErelocFailures_ atTarget measurement, monitored when failure on Handover request, with MME forward relocation, exceeded a threshold in the last 15 minute interval. This value computes the failure rate at the Target MME for the Handover procedure with MME relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Look at all the failure counters for the Handover procedure with MME relocation (at the Target MME) in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 24-204 WmmLSS_failedNumHOPathSwNewSgwRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedNumHOPathSwNewSgwRateExceeded (4281) Type: mmeAlarm Package: ltemme.WmmLSS_ failedNumHOPathSwNewSgwRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedNumHOPathSwNewSgwRateExceeded, indicates the value of VS.cpiHOwSGWrelocFailures measurement, monitored when failure on Handover Path Switch request, to a different Serving Gateway, exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Handover procedure without MME relocation and with SGW relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Look at all the failure counters for the Handover procedure without MME relocation and with SGW relocation in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 24-205 WmmLSS_failedNumHOPathSwSameSgwRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedNumHOPathSwSameSgwRateExceeded (4282) Type: mmeAlarm Package: ltemme.WmmLSS_ failedNumHOPathSwSameSgwRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedNumHOPathSwSameSgwRateExceeded, indicates the value of VS.cpiHOwNoRelocFailures measurement, monitored when failure on Handover Path Switch request, to same Serving Gateway, exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Handover procedure without MME relocation and without SGW relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Contact your Nokia support representative.		

Table 24-206 WmmLSS_failedNumHORequiredRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedNumHORequiredRateExceeded (4283) Type: mmeAlarm Package: ltemme.WmmLSS_ failedNumHORequiredRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedNumHORequiredRateExceeded, indicates the value of VS.cpiHOwMMErelocFailures_ atSource measurement, monitored when failure on Handover request, with MME relocation, exceeded a threshold in the last 15 minute interval. This value computes the failure rate at the source MME for the Handover procedure with MME relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Look at all the failure counters for the Handover procedure with MME relocation (at the Source MME) in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 24-207 WmmLSS_failedS1MMEconnEstRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedS1MMEconnEstRateExceeded (4284) Type: mmeAlarm Package: ltemme.WmmLSS_ failedS1MMEconnEstRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedS1MMEconnEstRateExceeded, indicates the value of VS.cpiS1MMEconnFailures measurement, monitored when failed S1MME Connect request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the eNB connection over S1-MME, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify PLMN or TAI provisioning data, via the MME provisioning GUI. After validation of the data, if the problem persists, contact your Nokia support representative.		

Table 24-208 WmmLSS_failedServiceReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_failedServiceReqsRateExceeded (4285) Type: mmeAlarm Package: ltemme.WmmLSS_ failedServiceReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedServiceReqsRateExceeded, indicates the value of cpiServiceRequestFailures measurement, monitored when failure on Service request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the UE Service Request procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Ensure the S11 links to the SGW are normal, using the link_cli command. If the links look normal, and the alarm persists, contact your Nokia support representative.		

Table 24-209 WmmLSS_failedTAURateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_failedTAURateExceeded (4286) Type: mmeAlarm Package: ltemme.WmmLSS_failedTAURateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedTAURateExceeded, indicates the value of VS.cpiTauFailures measurement, monitored when failure on Tracking Area Update request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the TAU procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Contact your Nokia support representative.		

Table 24-210 WmmLSS_failedUpdBearerReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedUpdBearerReqsRateExceeded (4287) Type: mmeAlarm Package: ltemme.WmmLSS_ failedUpdBearerReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedUpdBearerReqsRateExceeded, indicates the value of cpiUpdateBearerFailures measurement, monitored when failure on Update Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Update Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Ensure S11 links are normal, using the link_cli command. If the links are normal, and the alarm persists, contact your Nokia support representative.		

Table 24-211 WmmLSS_failedUpdDedBearerReqsRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ failedUpdDedBearerReqsRateExceeded (4288) Type: mmeAlarm Package: ltemme.WmmLSS_ failedUpdDedBearerReqsRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_failedUpdDedBearerReqsRateExceeded, indicates the value of VS. cpiUpdateDedicatedBearerFailures measurement, monitored when failure on Update Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Update Dedicated Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify that S11 links are normal, using the link_cli command. If links are normal, and the alarm persists, contact your Nokia support representative.		

Table 24-212 WmmLSS_fru

Alarm	Attributes	Applicable major release
Name: WmmLSS_fru (4289) Type: mmeAlarm Package: ltemme.WmmLSS_fru Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM fru procedure, failures that occur will result in the generation of FRU alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the FRU alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-213 WmmLSS_ggsnDnsError

Alarm	Attributes	Applicable major release
Name: WmmLSS_ggsnDnsError (4290) Type: mmeAlarm Package: ltemme.WmmLSS_ggsnDnsError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: GGSN DNS Selection unable to retrieve IP Address. This alarm must be manually cleared.		
Remedial action: Verify that the GGSN IP Address is provisioned correctly on DNS server.\nManually clear the alarm.		

Table 24-214 WmmLSS_grow

Alarm	Attributes	Applicable major release
Name: WmmLSS_grow (4291) Type: mmeAlarm Package: ltemme.WmmLSS_grow Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM grow procedure, failures that occur will result in the generation of GROW alarm.		

Table 24-214 WmmLSS_grow (continued)

Alarm	Attributes	Applicable major release
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the GROW alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-215 WmmLSS_hostDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_hostDown (4292) Type: mmeAlarm Package: ltemme.WmmLSS_hostDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A Service Host abnormally transitioned to an out-of-service state. (Note, this alarm will only be generated if the mate Service Host is in-service.)		
Remedial action: In general, the first few occurrences of the abnormal termination is automatically recovered by integrity software on the Service Host, in which case no manual action is necessary. When automatic recovery occurs the alarm clears automatically as well. However, if the unexpected event causing the abnormal termination occurs at a frequent enough rate, the Service Host can be left in a permanent Unavailable state. If in this state the alarm will not be cleared automatically and manual action is necessary to restore the Service Host. Bringing a Service Host software back to an In-Service state can be initiated from the MI.\nUltimately, the reason for the abnormal termination needs to be determined and a fix provided. Fortunately, debugging output is sent to the MI Log File and core files are typically generated when these conditions occur. To aid Nokia support in providing a fix, the storage of the MI Log File and the collection of any core files at the time the error occurred should be done and made available. The location of generated core files is /var/core on the Service host that experienced the abnormal termination.		

Table 24-216 WmmLSS_hostReset

Alarm	Attributes	Applicable major release
Name: WmmLSS_hostReset (8395) Type: mmeAlarm Package: ltemme.WmmLSS_hostReset Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The Redundancy Manager is requesting a host reset. This will occur when one or more services on a host do not initialize properly and local recovery attempts have been unsuccessful.		
Remedial action: No manual action is needed for this alarm. It will be cleared automatically when services start to initialize.		

Table 24-217 WmmLSS_internalCommunicationFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_internalCommunicationFailure (4293) Type: mmeAlarm Package: ltemme.WmmLSS_ internalCommunicationFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Communication between active MIF member and active MAF/SAF member failed or communications between active MIF member and active MPH member failed.		
Remedial action: Verfiy MPH, MIF and/or MAF have not been forced out-of-service.\nIf communication is lost between the MPH and the MIF and it does not come back automatically, and MPH pool is in Active / Hot-standby state, try switching MPH to the standby member.\nIf communication is lost between the MAF and the MIF and it does not come back automatically, and MAF pool is in Active / Hot-standby state, try switching MAF to the standby member.\nIf communication is lost between the MIF and MPH and the MIF and MAFs and it does not come back automatically, and MIF pool is in Active / Hot-standby state, try switching MIF to the standby member.		

Table 24-218 WmmLSS_ippuBusError

Alarm	Attributes	Applicable major release
Name: WmmLSS_ippuBusError (4294) Type: mmeAlarm Package: ltemme.WmmLSS_ippuBusError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: There is a bus error on the indicated host between the HSPP4 hardware (iPPU) in the AMC slot and the host hardware.		
Remedial action: Determine if any related alarms are also present, such as on the ESC, chassis, or board itself. Correct those alarms first and see if this alarm clears as a result.\nOn 9471 WMM: Utilize ippu_cli to print the status of the board on the OAM host.\nOn 9471 WMM: Verify the appropriate FRUID via shelf manager is present in the given ShelfId CardId.\nOn 9471 WMM: Visually verify HSPP4 hardware is present in the AMC slot of the alarm indicated with a ShelfId and cardId.\nOn 9471 WMM: On the Shelf Manager, verify the shelf and card in the alarm has an HSPP4 iPPU in the AMC slot. If HSPP4 is not detected, attempt to powercycle the card.\nOn 9471 WMM: On the Shelf Manager, verify the shelf and card in the alarm has an HSPP4 iPPU in the AMC slot. If HSPP4 is not detected, attempt to re-seat the card in the alarm by ShelfId and CardId.\nOn 9471 WMM: On the Shelf Manager, verify the shelf and card in the alarm has an HSPP4 iPPU in the AMC slot. If HSPP4 is not detected, replace the card used for this host using the appropriate FRU procedure as necessary.\nOn 9471 WMM: Attempt to reset the entire host (ShelfId/CardId) via appropriate CLI or MI. Before attempting this action, verify that there is an ACTIVE or STANDBY mate present in the system.\nIf the above steps do not clear the alarm, contact your Nokia support representative.		

Table 24-219 WmmLSS_ippuDegraded

Alarm	Attributes	Applicable major release
Name: WmmLSS_ippuDegraded (8049) Type: mmeAlarm Package: ltemme.WmmLSS_ippuDegraded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when the IPPU is either not working or incorrectly configured.		
Remedial action: Reboot the MAF blade hosting the IPPU. If the alarm persists after 30 minutes, contact your Nokia support representative.		

Table 24-220 WmmLSS_ippuResourceReset

Alarm	Attributes	Applicable major release
Name: WmmLSS_ippuResourceReset (4295) Type: mmeAlarm Package: ltemme.WmmLSS_ippuResourceReset Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: There was a software reset on the iPPU in the HSPP4 AMC or a restart by the PMB process in the host identified by ShelfId and CardId.		
Remedial action: Determine if any related alarms are present. Correct those alarms first and see if this alarm clears as a result.\nOn 9471 WMM: Utilize ippu_cli to print the status of the board on the OAM host.\nOn 9471 WMM: Before attempting this action, verify that there is an ACTIVE or STANDBY mate present in the system. Attempt to reset the entire card (shelf/slot) via appropriate CLI interface or MI.\nIf the above steps do not clear the alarm, contact your Nokia support representative.		

Table 24-221 WmmLSS_laiFqdnError

Alarm	Attributes	Applicable major release
Name: WmmLSS_laiFqdnError (8396) Type: mmeAlarm Package: ltemme.WmmLSS_laiFqdnError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: MME DNS Selection unable to retrieve SGW IP Address associated with FQDN. this alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.\nManually clear the alarm.		

Table 24-222 WmmLSS_liNearingCapacityLimit

Alarm	Attributes	Applicable major release
Name: WmmLSS_liNearingCapacityLimit (4296) Type: mmeAlarm Package: Itemme.WmmLSS_liNearingCapacityLimit Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The number of lawful interceptions has reached 80% of MAF/SAF capacity.		
Remedial action: Use the query option of the li_target_cli command to verify that the appropriate set of UEs are selected for lawful interception.		

Table 24-223 WmmLSS_logRotateThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_logRotateThreshold (10265) Type: mmeAlarm Package: Itemme.WmmLSS_logRotateThreshold Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 10.0.0 • 10.1.0
Description: A log file has exceeded the number of rotations that are expected. The name of the log file can be identified in the message field of the alarm. The log rotate threshold(normally 75%, such as 3 log rotate times reached while the total log rotate times is 4).		
Remedial action: If this alarm generated, customer need to pull/move the logs to their own server to avoid the log is overwritten as the rotate threshold reached.\nThis alarm must be manually cleared from the MI GUI or alarm_cli once the number of logs have been reduced to be below the log rotate threshold.\nIf the problem persists, contact your Nokia support representative.		

Table 24-224 WmmLSS_lostOfSDP

Alarm	Attributes	Applicable major release
Name: WmmLSS_lostOfSDP (5152) Type: mmeAlarm Package: Itemme.WmmLSS_lostOfSDP Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: SDP is operationally down.		
Remedial action: Check SDP configuration. Use sdp-ping to check accessibility far-end.\nManually clear the alarm.		

Table 24-225 WmmLSS_lostOfSpokeSDP

Alarm	Attributes	Applicable major release
Name: WmmLSS_lostOfSpokeSDP (5153) Type: mmeAlarm Package: ltemme.WmmLSS_lostOfSpokeSDP Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Spoke-SDP is operationally down.		
Remedial action: Check ingress and egress label mapping.\nManually clear the alarm.		

Table 24-226 WmmLSS_maxDurationExpiredOnHRPDhandover

Alarm	Attributes	Applicable major release
Name: WmmLSS_ maxDurationExpiredOnHRPDhandover (4297) Type: mmeAlarm Package: ltemme.WmmLSS_ maxDurationExpiredOnHRPDhandover Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_maxDurationExpiredOnHRPDhandover, indicates the value of VS.cpiMaxDurationHRPDhandover measurement, monitored when timed out on HRPD handover request exceeded a threshold in the last 15 minute interval. This value is the maximum time taken to perform a Handover to HRPD.		
Remedial action: Check the network routers for possible network delay. When the MME is programmed to include internal delay measurements, check these PMC values.		

Table 24-227 WmmLSS_memoryOverload

Alarm	Attributes	Applicable major release
Name: WmmLSS_memoryOverload (4298) Type: mmeAlarm Package: ltemme.WmmLSS_memoryOverload Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-227 WmmLSS_memoryOverload (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the memory utilization on a diskless service has exceeded a threshold or a memory allocation failure has occurred. The current default thresholds are: Minor - 80, Major - 85, Critical - 90.		
Remedial action: If memory usage regularly exceeds thresholds, investigate how the call traffic load can be reduced.\nIf it does not clear after step 1, contact your Nokia support representative to check if there is a memory leak occurring.		

Table 24-228 WmmLSS_mmeDnsError

Alarm	Attributes	Applicable major release
Name: WmmLSS_mmeDnsError (4299) Type: mmeAlarm Package: ltemme.WmmLSS_mmeDnsError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: MME DNS Selection unable to retrieve MME IP Address associated with FQDN. This alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.\nManually clear the alarm.		

Table 24-229 WmmLSS_msThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_msThreshold (4411) Type: mmeAlarm Package: ltemme.WmmLSS_msThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Number of attached MS or UE threshold reached		
Remedial action: If the problem persists, contact your Nokia support representative.		

Table 24-230 WmmLSS_nonCompliantFaultGroupMemberState

Alarm	Attributes	Applicable major release
Name: WmmLSS_ nonCompliantFaultGroupMemberState (8397) Type: mmeAlarm Package: ltemme.WmmLSS_ nonCompliantFaultGroupMemberState Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that a service member of a Fault Group is not in the same state as the rest of the members of that Fault Group. Because of that the Fault Group may become locked. If not corrected this can lead to issues with switching over services in that Fault Group.		
Remedial action: REM will attempt to correct the situation itself. If REM is unable to correct the situation Technical Support will need to be contacted for further analysis.		

Table 24-231 WmmLSS_noResetAckReceived

Alarm	Attributes	Applicable major release
Name: WmmLSS_noResetAckReceived (4305) Type: mmeAlarm Package: ltemme.WmmLSS_noResetAckReceived Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: No RESET ACKNOWLEDGEMENT message was received from the RNC after the WMM has sent and resent a RESET message.		
Remedial action: Verify the RNC that WMM fails to get the message from with is in service.\nDetermine that there are no errors within the IP network.		

Table 24-232 WmmLSS_nseBandwidthThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_nseBandwidthThreshold (4412) Type: mmeAlarm Package: ltemme.WmmLSS_nseBandwidthThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: NSE bandwidth threshold reached		

Table 24-232 WmmLSS_nseBandwidthThreshold (continued)

Alarm	Attributes	Applicable major release
Remedial action: Analyze the operation context of the alarm. Determine if this alarm is structural or conjectural.\nAnalyze the figures reported by the observation counters to evaluate how quick the NSE bandwidth has increased.Depending on the result of the investigations:\nIf the NSE bandwidth remains over this threshold most of the time, and if alarm with major severity also appears, upgrade of the SGSN configuration must be performed. Please contact your Nokia support representative.		

Table 24-233 WmmLSS_numberOfTuplesInUse

Alarm	Attributes	Applicable major release
Name: WmmLSS_numberOfTuplesInUse (4309) Type: mmeAlarm Package: Itemme.WmmLSS_numberOfTuplesInUse Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_numberOfTuplesInUse indicates that the number of tuples currently in use in a DA (data access) table used to store dynamic database information, has reached a threshold. The DA table in question is specified in the 'Resource'. The threshold is indicated in the 'Additional Information'.		
Remedial action: Contact your Nokia support representative.		

Table 24-234 WmmLSS_numTOS10gtpcRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_numTOS10gtpcRateExceeded (4306) Type: mmeAlarm Package: Itemme.WmmLSS_numTOS10gtpcRateExceeded Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_numTOS10gtpcRateExceeded, indicates the value of VS.cpiGTPcResponseTO_S10 measurement, monitored when missing replies to S10(gtpc) request exceeded a threshold in the last 15 minute interval. This value computes the cpiage of Response messages that are not received over S10, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Check the network routers for any problems. Check to determine if any other MME elements are having problems.		

Table 24-235 WmmLSS_numTOS11gtpcRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_numTOS11gtpcRateExceeded (4307) Type: mmeAlarm Package: ltemme.WmmLSS_ numTOS11gtpcRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_numTOS11gtpcRateExceeded, indicates the value of VS.cpiGTPcResponseTO_S11 measurement, monitored when missing replies to S11(gtpc) request exceeded a threshold in the last 15 minute interval. This value computes the cpiage of Response messages that are not received over S11, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify that S11 links are normal, using the link_cli command. If links are normal, and the alarm persists, contact your Nokia support representative.		

Table 24-236 WmmLSS_numTOS3gtpcRateExceeded

Alarm	Attributes	Applicable major release
Name: WmmLSS_numTOS3gtpcRateExceeded (4308) Type: mmeAlarm Package: ltemme.WmmLSS_ numTOS3gtpcRateExceeded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm, LSS_numTOS3gtpcRateExceeded, indicates the value of VS.numTOS3gtpcRateExceeded measurement, monitored when missing replies to S3(gtpc) request exceeded a threshold in the last 5 minute interval. This value computes the percentage of Response messages that are not received over S3, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.		
Remedial action: Verify that S3 links are normal, using the link_cli command. If links are normal, and the alarm persists, contact your Nokia support representative.		

Table 24-237 WmmLSS_osSecInfoModificationDetected

Alarm	Attributes	Applicable major release
Name: WmmLSS_osSecInfoModificationDetected (4310) Type: mmeAlarm Package: ltemme.WmmLSS_osSecInfoModificationDetected Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that an unexpected modification on the security information of a host operating system has been detected by the security audit program.		
Remedial action: Access MI GUI for the detailed information of this security alarm.\nInvestigate the problematic file identified in the additionalText string. Correct any errors found during the investigation the problem. Contact your Nokia support representative as needed.\nOnce the error has been corrected, clear the alarm from the MI GUI.		

Table 24-238 WmmLSS_osSecInformationMissing

Alarm	Attributes	Applicable major release
Name: WmmLSS_osSecInformationMissing (4311) Type: mmeAlarm Package: ltemme.WmmLSS_osSecInformationMissing Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the security information Golden copy of a host operating system has been deleted. The Golden copy is the initial snapshot of the host operating system, which is used by the security audit program to identify possible security violations of the host operating system.		
Remedial action: Access MI GUI for the detailed information of this security alarm.\nInvestigate the problematic file identified in the additionalText string. Correct the problem by performing a Security Audit on this host from MI GUI to re-create the Golden copy. Contact your Nokia support representative as needed.\nOnce the error has been corrected, clear the alarm from MI GUI.		

Table 24-239 WmmLSS_osSecUnexpectedInformation

Alarm	Attributes	Applicable major release
Name: WmmLSS_osSecUnexpectedInformation (4312) Type: mmeAlarm Package: ltemme.WmmLSS_osSecUnexpectedInformation Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that security audit program has detected an unexpected program currently running on a host.		
Remedial action: First access MI GUI for the detailed information about this security alarm. Investigation is needed to find out how the offending service/program got installed. The alarm can be manually cleared after removing the service/program and verifying the system integrity.		

Table 24-240 WmmLSS_patch

Alarm	Attributes	Applicable major release
Name: WmmLSS_patch (4313) Type: mmeAlarm Package: ltemme.WmmLSS_patch Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0
Description: When performing SIM patch procedure, failures that occur will result in the generation of PATCH alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the PATCH alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-241 WmmLSS_pathAvailability

Alarm	Attributes	Applicable major release
Name: WmmLSS_pathAvailability (4314) Type: mmeAlarm Package: ltemme.WmmLSS_pathAvailability Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-241 WmmLSS_pathAvailability (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when SCTP path becomes unavailable. The local and remote provisioned addresses need to be checked for use of the correct 2 sub-networks provided. If the provisioned addresses match the 2 physical subnets, and if all address provisioned are also correct, then the physical network that carries the subnet used in the path 'unavailable' alarm needs to be investigated for trouble. The specifics of the path are documented in the 'additionalText' field of the alarm. These alarms may need to be cleared manually: as alarms are reported when path connectivity is established, however their contents are a function of provisioned addresses (paths) that may be wrong and changed when the connection is down, and may no longer match with the path that was originally alarmed.		
Remedial action: Verify that the endpoints IP addresses on the MME are the remote entity are provisioned correctly.\nVerify that the network between the MME and the remote entity is functioning correctly.		

Table 24-242 WmmLSS_pdpThreshold

Alarm	Attributes	Applicable major release
Name: WmmLSS_pdpThreshold (4413) Type: mmeAlarm Package: ltemme.WmmLSS_pdpThreshold Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Number of activated PDP context threshold reached.		
Remedial action: Analyze the operation context of the alarm. Determine if this alarm is structural or conjectural.\nAnalyze the observation counters values to evaluate how quick the number of activated PDP contexts has increased. Depending on the result of the investigations:\nIf the activated PDP contexts overload corresponds to a specific peak, you don't need to perform any upgrade of the SGSN. If alarm LSS_pdpThreshold is present as major, the activated PDP contexts overload is constant. There is a gap between the demand of PS services and the SGSN processing capacity. You need to upgrade the SGSN configuration. Please contact your Nokia support representative.		

Table 24-243 WmmLSS_pgwDnsError

Alarm	Attributes	Applicable major release
Name: WmmLSS_pgwDnsError (4315) Type: mmeAlarm Package: ltemme.WmmLSS_pgwDnsError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: MME DNS Selection unable to retrieve PGW IP Address associated with FQDN. This alarm must be manually cleared.		

Table 24-243 WmmLSS_pgwDnsError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.\nManually clear the alarm.		

Table 24-244 WmmLSS_pktCorruptionDetectedViaRCCLANCheck

Alarm	Attributes	Applicable major release
Name: WmmLSS_ pktCorruptionDetectedViaRCCLANCheck (4316) Type: mmeAlarm Package: ltemme.WmmLSS_ pktCorruptionDetectedViaRCCLANCheck Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The LANCHECK audit has identified corrupted packets being transmitted through the network.		
Remedial action: The reason for the data corruption needs to be understood and corrected. It is possible that the Service Host Ethernet Port failed, the cabling that interconnects the Ethernet Port to the network is damaged, the Routers and/or Ethernet Switches that make up the SoftSwitch Network failed. Investigate each of these reasons and discount or correct. Once corrected, the alarm will be cleared.		

Table 24-245 WmmLSS_platformCommandFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_platformCommandFailure (4317) Type: mmeAlarm Package: ltemme.WmmLSS_platformCommandFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that a linux command started via crond has failed to execute on a host.		
Remedial action: Access MI GUI for the detailed information of this security alarm.\nInvestigate the specific offending file identified in additionalText string and correct the problem. Contact your Nokia support representative as needed.\nOnce the file has been corrected, clear the alarm from the MI GUI.		

Table 24-246 WmmLSS_pmDataNotCollected

Alarm	Attributes	Applicable major release
Name: WmmLSS_pmDataNotCollected (4318) Type: mmeAlarm Package: ltemme.WmmLSS_pmDataNotCollected Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised alarm LSS_pmDataNotCollected indicates that the PM process on CNFG card could not receive PM data from a service in a interval(5 minutes).		
Remedial action: Check if the card is in the network congestion status. if it could not be pinged through, please restart the card.\nCheck if the card is in the init status. if yes, please wait for a while.\nIf the above steps do not correct the problem, contact your Nokia support representative.		

Table 24-247 WmmLSS_processDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_processDown (4319) Type: mmeAlarm Package: ltemme.WmmLSS_processDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that an application process that should be running has terminated.		
Remedial action: Recovery software should automatically recover from the abnormal or maintenance event that has caused the process termination, without any manual involvement. The automatic recovery will restart just that process or will reboot the card as necessary.\nIf the alarm does not clear or if it occurs repeatedly, contact your Nokia support representative.		

Table 24-248 WmmLSS_processNotStarted

Alarm	Attributes	Applicable major release
Name: WmmLSS_processNotStarted (4320) Type: mmeAlarm Package: ltemme.WmmLSS_processNotStarted Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm is LSS_processNotStarted as raised by the MME system		
Remedial action: IPM: Based on the type of failure encountered, recovery actions may vary. If the ipmStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the ipm process will automatically clear the alarm.\nDHCPD: Based on the type of failure encountered, recovery actions vary. If the dhcpdStartupFailure is generated, contact your Nokia support representative. Once the failure is correct, the startup of the dhcpd process will automatically clear the alarm.\ nDNSPROXY: Based on the type of failure encountered, recovery actions may vary. If the dnsproxyStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the dnsproxy process will automatically clear the alarm.\nPDNS SERVER: Based on the type of failure encountered, recovery actions may vary. If the pdnsStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the pdns process will automatically clear the alarm.\nUNBOUND: Based on the type of failure encountered, recovery actions may vary. If the unboundStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the unbound process will automatically clear the alarm.\nLIGHTTPD: Based on the type of failure encountered, recovery actions may vary. If the lighttpdStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the lighttpd process will automatically clear the alarm.\nSSHD: Based on the type of failure encountered, recovery actions may vary. If the sshdStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the sshd process will automatically clear the alarm.\nNTPD: Based on the type of failure encountered, recovery actions may vary. If the ntpdStartupFailure is generated, contact your Nokia support representative. Once the failure is corrected, the startup of the ntpd process will automatically clear the alarm.		

Table 24-249 WmmLSS_provisioningError

Alarm	Attributes	Applicable major release
Name: WmmLSS_provisioningError (4321) Type: mmeAlarm Package: ltemme.WmmLSS_provisioningError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Missing provisioning of TAI-to-LAI mapping to MSC in 2G/3G operator for SGS based CSFB/SMS.		
Remedial action: Provision missing entries in TAI-LAI mapping table utilizing LAI in 2G/3G operator. Refer to user text in alarm.		

Table 24-250 WmmLSS_remotedbLinkDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_remotedbLinkDown (4323) Type: mmeAlarm Package: ltemme.WmmLSS_remotedbLinkDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm will be displayed when the remotedb trigger function connection does not exist.		
Remedial action: Normally the alarm will be cleared automatically when a remote service restarts and re-connects to the remotedb database; If this alarm is not cleared, please contact your Nokia support representative.		

Table 24-251 WmmLSS_remoteQueryServerFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_remoteQueryServerFailure (4322) Type: mmeAlarm Package: ltemme.WmmLSS_ remoteQueryServerFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that a host has lost connection to a remote DNS/ENUM server.		
Remedial action: The user needs to check the failed DNS server as to the nature of the server failure		

Table 24-252 WmmLSS_restore

Alarm	Attributes	Applicable major release
Name: WmmLSS_restore (4324) Type: mmeAlarm Package: ltemme.WmmLSS_restore Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM restore procedure, failures that occur will result in the generation of RESTORE alarm.		

Table 24-252 WmmLSS_restore (continued)

Alarm	Attributes	Applicable major release
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the RESTORE alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-253 WmmLSS_serviceCFGDataTimestampError

Alarm	Attributes	Applicable major release
Name: WmmLSS_serviceCFGDataTimestampError (10266) Type: mmeAlarm Package: ltemme.WmmLSS_serviceCFGDataTimestampError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 10.0.0 • 10.1.0
Description: A mismatch in the configuration timestamp has been detected between the configuration server and the service indicated in the alarm.		
Remedial action: For the REM controlled services, with the exception of IWF, NGSS, and FS5K, the associated service pool must be initialized to clear this alarm. The IWF, NGSS, and FS5K can be recovered by switching the service (promoting the standby side to active). For the other services, the state of the service needs to be assessed prior to taking recovery. If the service is working without any observable failures, the duplex recovery should be scheduled in off hours to minimize service impacts from the initialization. Otherwise, the service should be initialized, which will result in a duplex failure.\nContact your Nokia support representative		

Table 24-254 WmmLSS_serviceOnewayCommunication

Alarm	Attributes	Applicable major release
Name: WmmLSS_serviceOnewayCommunication (4325) Type: mmeAlarm Package: ltemme.WmmLSS_serviceOnewayCommunication Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A service might have one way communication to the Redundancy Manager and possibly other network elements.		
Remedial action: Wait approximately 1 minute 30 seconds; if the alarm does not clear autonomously, one will need to investigate why the alarm does not clear.\nCheck and see if there are other outstanding alarms on this service that might trump the onewayCommunication alarm. Those alarms would be of type connectionLost; or any other alarms associated to the state of the service. Other alarms would indicate that a more severe problem exists on the service; and onewayCommunication could optionally be cleared at this point; as the other service based alarms most likely supersede the onewayCommunication alarm.		

Table 24-255 WmmLSS_sgsnDnsError

Alarm	Attributes	Applicable major release
Name: WmmLSS_sgsnDnsError (4326) Type: mmeAlarm Package: ltemme.WmmLSS_sgsnDnsError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: SGSN DNS Selection unable to retrieve SGSN IP Address associated with FQDN. This alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.\nManually clear the alarm.		

Table 24-256 WmmLSS_sgwResourceDegraded

Alarm	Attributes	Applicable major release
Name: WmmLSS_sgwResourceDegraded (8050) Type: mmeAlarm Package: ltemme.WmmLSS_sgwResourceDegraded Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The raised LSS_sgwResourceDegraded alarm indicates the WMM selection on SGW or SGW-PGW pair has been degraded.		
Remedial action: Determine that there are no errors within the IP network.\nDetermine that the SGW and/or SGW PGW pair are in service.\nCheck if the invocation of wmm_cli tool was intentional.		

Table 24-257 WmmLSS_sgwSelectionFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_sgwSelectionFailure (5106) Type: mmeAlarm Package: ltemme.WmmLSS_sgwSelectionFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0
Description: SGSN fails to select a SGW either due to failure to select SGW S5 service, SGW S8 service, or SGW S4 service. This alarm shall be manually cleared.		
Remedial action: Verfiy that the SGW is provisioned, configured correctly.\nManually clear the alarm.		

Table 24-258 WmmLSS_sheddingOverload

Alarm	Attributes	Applicable major release
Name: WmmLSS_sheddingOverload (4327) Type: mmeAlarm Package: ltemme.WmmLSS_sheddingOverload Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates the message shedding severity under system overload. The two severity levels indicate the degree of shedding severity. The types of messages/calls that are shed is specific to the application and there tends to be additional types of messages impacted by the shedding as the severity increases. Currently the default thresholds between Major and Critical is 70.		
Remedial action: Verify that there is no running debug or testing tool that uses a lot of CPU/memory.\nIf CPU or memory utilization regularly exceeds thresholds, investigate how the call traffic load can be reduced:\nReengineer so less traffic is directed to this office or card.\nConsider replacing the overloaded card pair with higher-capacity cards.\nVerify if there are enough cards to handle the expected load and add additional cards as appropriate.		

Table 24-259 WmmLSS_shmcEthernetError

Alarm	Attributes	Applicable major release
Name: WmmLSS_shmcEthernetError (4328) Type: mmeAlarm Package: ltemme.WmmLSS_shmcEthernetError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The Ethernet link to the Shelf Management Card (ShMC) has failed.		
Remedial action: Verify the hub port corresponding to this server by telnet to the hub card. Correct or replace the hub as necessary.\nVerify that the shelf management cards are running on active/standby status by 'clia shmstatus' command on shelf management card. Correct the status as necessary.		

Table 24-260 WmmLSS_simxml

Alarm	Attributes	Applicable major release
Name: WmmLSS_simxml (4329) Type: mmeAlarm Package: ltemme.WmmLSS_simxml Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing simxml procedure, failures that occur will result in the generation of SIMXML alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the SIMXML alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-261 WmmLSS_softwareAllocatedResourceOverload

Alarm	Attributes	Applicable major release
Name: WmmLSS_ softwareAllocatedResourceOverload (4330) Type: mmeAlarm Package: ltemme.WmmLSS_ softwareAllocatedResourceOverload Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates that the utilization of a pre-allocated resource by software has exceeded thresholds. The resource could be internal buffer, data structure array, table entries, etc.		
Remedial action: Consider reengineering so that less traffic is directed to this service.\nIf condition persists, contact your Nokia support representative.		

Table 24-262 WmmLSS_softwareComponentDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_softwareComponentDown (5145) Type: mmeAlarm Package: ltemme.WmmLSS_ softwareComponentDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-262 WmmLSS_softwareComponentDown (continued)

Alarm	Attributes	Applicable major release
Description: Software that is executing on the Service Host has terminated abnormally.		
Remedial action: Generally, no manual action is necessary.\nIntegrity software on the Service Host takes care of automatic recovery from the abnormal termination. When automatic recovery occurs the alarm will be cleared automatically as well.\nThe affected software gets in a permanent unavailable state after frequent abnormal terminations. In this state, the alarm will not be cleared automatically and manual action will be necessary to restore the software.\nBringing Service Host software back to an in-service state can be initiated from the MI. Use the MI GUI virtual host screen, initialization control option.\nIf the problem reoccurs, contact your Nokia support representative.		

Table 24-263 WmmLSS_softwareComponentStandbyNotReady

Alarm	Attributes	Applicable major release
Name: WmmLSS_ softwareComponentStandbyNotReady (4331) Type: mmeAlarm Package: ltemme.WmmLSS_ softwareComponentStandbyNotReady Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The state of the software component, Virtual Machine (VM) that is executing on the Service Host is standby-cold or standby-cool		
Remedial action: Generally, no manual action is necessary. Integrity software on the Service Host takes care of automatic recovery from the standby-cold/standby-cool state. When automatic recovery occurs the alarm clears automatically as well. The timing for each VM to come up is different. Since this alarm will fire during the NORMAL init time, it should not treat as a problem until 10 minutes later.\nIf the alarm does not clear after one interval, contact your Nokia support representative.		

Table 24-264 WmmLSS_svcdegrow

Alarm	Attributes	Applicable major release
Name: WmmLSS_svcdegrow (4332) Type: mmeAlarm Package: ltemme.WmmLSS_svcdegrow Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM service degrow (svcdegrow) procedure, failures that occur will result in the generation of SVCDEGROW alarm.		

Table 24-264 WmmLSS_svcdegrow (continued)

Alarm	Attributes	Applicable major release
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the SVCDEGROW alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-265 WmmLSS_svcgrow

Alarm	Attributes	Applicable major release
Name: WmmLSS_svcgrow (4333) Type: mmeAlarm Package: ltemme.WmmLSS_svcgrow Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing SIM service grow (svcgrow) procedure, failures that occur will result in the generation of SVCGROW alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the SVCGROW alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resumption of the SIM procedures will automatically clear the alarm.		

Table 24-266 WmmLSS_swVersionMismatch

Alarm	Attributes	Applicable major release
Name: WmmLSS_swVersionMismatch (4334) Type: mmeAlarm Package: ltemme.WmmLSS_swVersionMismatch Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The software version running on this service member does not match the version that should be running according to the database table IPCFG_POOL_MEMBERS, field build_sec.		
Remedial action: On the MI, run the remVersCheck command. It should show that for this service member, build_sec disagrees between the database and the running binary. Check whether either of them agrees with the service zip file.\nIf the database and zip agree, initialize the service member. Otherwise, contact your Nokia support representative.		

Table 24-267 WmmLSS_taiFqdnError

Alarm	Attributes	Applicable major release
Name: WmmLSS_taiFqdnError (4335) Type: mmeAlarm Package: ltemme.WmmLSS_taiFqdnError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: MME DNS Selection unable to retrieve SGW IP Address associated with FQDN. this alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.\nManually clear the alarm.		

Table 24-268 WmmLSS_tftpDownloadCorrupt

Alarm	Attributes	Applicable major release
Name: WmmLSS_tftpDownloadCorrupt (4336) Type: mmeAlarm Package: ltemme.WmmLSS_tftpDownloadCorrupt Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm can be fired due to two different problems. Alarm information is given specific sub-section below.		
Remedial action: If the Additional Info field looks like TftpOpen() Failure Ret(hexadecimal error number), IORet(hexadecimal error number), File(service application zip file name and path), IP(hexadecimal version of the CNFG host IP) continue on to step 2. Otherwise, go to step 3.\nCheck the file name and path on the indicated CNFG host and ensure that is readable by all. If not performing SU or Path, recover file from mate CNFG host.\nreboot the host issuing the alarm\nIf the alarm persists. Contact your Nokia support representative.		

Table 24-269 WmmLSS_threadsExhausted

Alarm	Attributes	Applicable major release
Name: WmmLSS_threadsExhausted (5111) Type: mmeAlarm Package: ltemme.WmmLSS_threadsExhausted Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-269 WmmLSS_threadsExhausted (continued)

Alarm	Attributes	Applicable major release
Description: One or more critical CP Tasks have been un-responsive to regular Integrity Monitor - IMON Heartbeats. IMON attempted to restart them and multiple restarts have escalated to a Process Init on the Standby Card or a Switch Over to the Standby Card from the Active Card where the target stuck task was running.		
Remedial action: NOT APPLICABLE		

Table 24-270 WmmLSS_upgrade

Alarm	Attributes	Applicable major release
Name: WmmLSS_upgrade (4337) Type: mmeAlarm Package: ltemme.WmmLSS_upgrade Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: When performing Software Upgrade (SU) related activities (which includes bkupSys and SIM upgrade procedure), failures that occur will result in generation of SU alarm.		
Remedial action: Based on the type of failure encountered, recovery actions may vary. If the SU alarm is generated, contact your Nokia support representative. Once the failure is corrected, a resume of the SIM procedures will automatically clear the alarm. For bkupSys, once the failure is corrected re-executing bkupSys will automatically clear the alarm.		

Table 24-271 WmmLSS_virtualClusterDown

Alarm	Attributes	Applicable major release
Name: WmmLSS_virtualClusterDown (4338) Type: mmeAlarm Package: ltemme.WmmLSS_virtualClusterDown Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A Virtual Cluster spanning a pair of Service Hosts abnormally transitioned to an out-of-service state. (Note, a Virtual Cluster is a logical grouping of a pair of Software Components. Each Software Component executes on a separate Service Host and typically runs Active and Standby.)		
Remedial action: If this alarm persists, contact your Nokia support representative.		

Table 24-272 WmmLSS_wmmExcessiveExtCommFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_wmmExcessiveExtCommFailure (9564) Type: mmeAlarm Package: ltemme.WmmLSS_wmmExcessiveExtCommFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.1.0 • 10.0.0 • 10.1.0
Description: An excessive number of network elements of a given type (e.g. RNC) are having communication failure with the WMM. This is usually due to a network connectivity problem and not the individual external network element. Once this alarm is triggered the WMM will stop reporting alarms for the network element of the given type. Once the network problem is resolved and the alarm no longer excessive, this alarm will clear. This alarm is raised when at least 100 network elements of a given type having communication failure. This alarm clears when 95 or fewer are having communication failure.		
Remedial action: Determine that there are no errors within the IP network.\nIf the network entity data is provisioned on WMM, verify the data is correct.\nVerify the network entity that WMM fails to communicate with is in service.		

Table 24-273 WmmLSS_wmmExternalCommFailure

Alarm	Attributes	Applicable major release
Name: WmmLSS_wmmExternalCommFailure (9565) Type: mmeAlarm Package: ltemme.WmmLSS_wmmExternalCommFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.1.0 • 10.0.0 • 10.1.0
Description: Communication between WMM and another network entity can not be established. The additional text field indiactes the specific entity involved.		
Remedial action: Verify the network entity that WMM fails to communicate with is in service.\nDetermine that there are no errors within the IP network.\nIf the network entity data is provisioned on WMM, verify the data is correct.\nIf multiple links that terminate on the MIF are down, try switching MIF to hot-standby mate.\nIf multiple links that terminate on the MPH are down, try switching MPH to hot-standby mate.		

Table 24-274 WmmLSS_wmmLicenseKeyExpiration

Alarm	Attributes	Applicable major release
Name: WmmLSS_wmmLicenseKeyExpiration (8398) Type: mmeAlarm Package: ltemme.WmmLSS_wmmLicenseKeyExpiration Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: License has expired.		

Table 24-274 WmmLSS_wmmLicenseKeyExpiration (continued)

Alarm	Attributes	Applicable major release
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (NSLM).\nTransfer and Install license file: Create a staging /storage/TEMP directory with following command if it does not exist. mkdir -m755 -p /storage/TEMP Transfer the obtained license file named 'license' to the staging /storage/TEMP directory in both OAM side-A and side-B. Install the staged license file by logging on as root to both side-A and side-B using the following commands: mkdir -p /storage/lic/ cp /storage/TEMP/license /storage/lic/ chmod 500 /storage/lic/license\nUnlock system running WMM on HP C7000 or WMM on VMM: If the LSS_wmmLicenseKeyValidationError or the LSS_ wmmLicenseKeyExpiration alarm is outstanding for more than 60 minutes, the licensing enforcement has locked the WMM system. The following command must be performed to unlock the system. The corresponding alarm will clear after the successful execution of the unlock request. For SRS application use rsm_cli -o unlock -e srsaggsvc otherwise use rsm_cli -o unlock -e mmeaggsvc If the above command execution has no output, it indicates the newly installed license is valid and the unlock request of MME/SRS aggregate service was successful. If the above command execution has the following output: 'rsm_cli RSM result: Aggregate service unlock request denied due to missing or invalid license file' then the installed license file is still invalid. Verify if step 1 and 2 were done correctly. Verify if the licensed system ID in the license file matches the provisioned system ID. If the above command execution has the following output: 'rsm_cli RSM result: UELB CLI (tools perform ue-loadbalancing) has locked the WMM. Can not execute requested command' then the installed license file is valid now, but the UELB procedure was performed and also locked the MME/SRS aggregate service. Perform UELB unlock MME/SRS aggregate service admin state via wmm_cli: tools perform ue-loadbalancing shutdown		

Table 24-275 WmmLSS_wmmLicenseKeyNearExpiration

Alarm	Attributes	Applicable major release
Name: WmmLSS_wmmLicenseKeyNearExpiration (8399) Type: mmeAlarm Package: ltemme.WmmLSS_ wmmLicenseKeyNearExpiration Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: License is near expiration. If the license's expiration is within 30 days, a minor alarm is raised. If the license's expiration is within 14 days, a major alarm is raised. If the license's expiration is within 3 days, a critical alarm is raised.		
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (NSLM).\nTransfer and Install license file: Create a staging /storage/TEMP directory with following command if it does not exist. mkdir -m755 -p /storage/TEMP Transfer the obtained license file named 'license' to the staging /storage/TEMP directory in both OAM side-A and side-B. Install the staged license file by logging on as root to both side-A and side-B using the following commands: mkdir -p /storage/lic/ cp /storage/TEMP/license /storage/lic/ chmod 500 /storage/lic/license		

Table 24-276 WmmLSS_wmmLicenseKeyValidationError

Alarm	Attributes	Applicable major release
Name: WmmLSS_wmmLicenseKeyValidationError (8400) Type: mmeAlarm Package: ltemme.WmmLSS_ wmmLicenseKeyValidationError Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: License file is missing or invalid.		

Table 24-276 WmmLSS_wmmLicenseKeyValidationError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Obtain license file: Please contact your Nokia support or sales representative for assistance with obtaining a license file from Nokia Software License Manager (NSLM).\nTransfer and Install license file: Create a staging /storage/TEMP directory with following command if it does not exist. mkdir -m755 -p /storage/TEMP Transfer the obtained license file named 'license' to the staging /storage/TEMP directory in both OAM side-A and side-B. Install the staged license file by logging on as root to both side-A and side-B using the following commands: mkdir -p /storage/lic/ cp /storage/TEMP/license /storage/lic/ chmod 500 /storage/lic/license\nUnlock system running WMM on HP C7000 or WMM on VMM: If the LSS_wmmLicenseKeyValidationError or the LSS_ wmmLicenseKeyExpiration alarm is outstanding for more than 60 minutes, the licensing enforcement has locked the WMM system. The following command must be performed to unlock the system. The corresponding alarm will clear after the successful execution of the unlock request. For SRS application use rsm_cli -o unlock -e srsaggsvc otherwise use rsm_cli -o unlock -e mmeaggsvc If the above command execution has no output, it indicates the newly installed license is valid and the unlock request of MME/SRS aggregate service was successful. If the above command execution has the following output: 'rsm_cli RSM result: Aggregate service unlock request denied due to missing or invalid license file' then the installed license file is still invalid. Verify if step 1 and 2 were done correctly. Verify if the licensed system ID in the license file matches the provisioned system ID. If the above command execution has the following output: 'rsm_cli RSM result: UELB CLI (tools perform ue-loadbalancing) has locked the WMM. Can not execute requested command' then the installed license file is valid now, but the UELB procedure was performed and also locked the MME/SRS aggregate service. Perform UELB unlock MME/SRS aggregate service admin state via wmm_cli: tools perform ue-loadbalancing shutdown		

Table 24-277 WMMPMFileNotificationMissing

Alarm	Attributes	Applicable major release
Name: WMMPMFileNotificationMissing (5387) Type: communicationsAlarm Package: Itemme.WMMPMFileNotificationMissing Raised on class: Itemme.MmeInstance	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PMFileNotificationMissing	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when a PM File notification is expected from the node, but has not been received after a certain period of time.		
Remedial action: SAM has not received a PM File notification from the node, and may have missed retrieving PM Files. Ensure that the node has PMEnabled and PMFileEvent values set to true. Ensure a PM job is active with an intended schedule. If the problem persists please contact your Nokia support representative for assistance. This alarm notification can be turned off under the General tab in the MME Instance.		

Table 24-278 WmmRALARM_Loop

Alarm	Attributes	Applicable major release
Name: WmmRALARM_Loop (4339) Type: mmeAlarm Package: ltemme.WmmRALARM_Loop Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm is RALARM_Loop as raised by the MME system		
Remedial action: loop 1 - Verify/replace circuit breakers/fuses.\nloop 2 - Depends on what device (e.g. temperature sensor) is connected to the external input.\nloops unavailable - contact your Nokia support representative.\nIf the problem persists, contact your Nokia support representative.		

Table 24-279 WmmRALARM_Power

Alarm	Attributes	Applicable major release
Name: WmmRALARM_Power (4340) Type: mmeAlarm Package: ltemme.WmmRALARM_Power Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm indicates a problem with the -48V, A feed or B feed, power to the Power Distribution Unit.		
Remedial action: Check the Power Distribution Units LEDs, circuit breakers, fuses, and power feeds.\nReplace the faulty alarm card, circuit breakers, fuses, or power feeds.\nIf the problem persists, contact your Nokia support representative.		

Table 24-280 WMMSnapshotException

Alarm	Attributes	Applicable major release
Name: WMMSnapshotException (10272) Type: communicationsAlarm Package: ltemme.WMMSnapshotException Raised on class: ltemme.WmmSnapshot	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: WMMSnapshotException	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: This alarm is raised when a probable corrupted file could not be deleted when performing a snapshot.		
Remedial action: An error was ecountered while performing WMM Snapshot. Certain files have not been creeated.		

Table 24-281 WmmSYS_BackupFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_BackupFailure (4341) Type: mmeAlarm Package: ltemme.WmmSYS_BackupFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The backup of an SNE has failed. On the next successful backup, this alarm will clear.		
Remedial action: If the additionalText of the alarm states 'Fail to get AccessKey for ESCHost/LNG application...', you need to set up userid/password on corresponding esc/lng in 'Configuration Management' --> 'Backup Management' --> 'Login Administration' panel on MI GUI first.\nAttempt another backup.\nIf the problem persists, contact your Nokia support representative.		

Table 24-282 WmmSYS_Configuration

Alarm	Attributes	Applicable major release
Name: WmmSYS_Configuration (4344) Type: mmeAlarm Package: ltemme.WmmSYS_Configuration Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-282 WmmSYS_Configuration (continued)

Alarm	Attributes	Applicable major release
Description: A possible configuration problem has been detected on the MI.		
Remedial action: If the specificProblem is MissingScheduledBackups: Run mi_audit -a sched_backups on the active MI to get a list of the devices that do not have a scheduled backup. For those devices, schedule a backup job using the MI GUI, Configuration Management->Backup Management->Scheduling Run mi_audit -a sched_backups on the active MI to clear the alarm once all required backups are scheduled.\nIf the specificProblem is PMDisabled: Run PMcontrol --master start on the active MI to enable PM collection This will enable PM collection on the MI and automatically clear this alarm.\nIf the specificProblem is NTPServerNotConfigured: Configure at least one NTP server. For ATCA, to add and configure an NTP server, refer to the section 'To add or delete remote NTP servers IP addresses' in the 5400 Linux Control Platform Configuration Management, 270-702-014 and 'To setup secure NTP configuration' in the 5400 Linux Control Platform Security Management, 270-702-015. For CPSB, to add and configure an NTP server, refer to the section 'To add or delete NTP server IP address' and 'Setup secure NTP configuration' in the Control Platform 1800 Operations, Administration, Maintenance and Provisioning, 270-900-872. Run mi_audit -a ntp on the active MI to clear the alarm.\nIf the specificProblem is NTPServerNotReachable: Run ntpconf_adm --action show_server to see the configured NTP server IP address(es). Resolve the connectivity problem to the intended NTP server. The NTP server should be pingable from the MI. Run mi_audit -a ntp on the active MI to clear the alarm.\nIf the specificProblem is MaintModeEnabled: This alarm will be raised when the MI is placed into maintenance mode for any maintenance activity using the mi_maint on cmd. It will be cleared when taken out of maintenance mode, using the mi_maint off cmd. If for some reason the alarm is not cleared and the maintenance flag is off (verify with mi_maint status cmd), run mi_audit -a maint_mode on the active MI to clear the alarm.		

Table 24-283 WmmSYS_CPM_USERDATA_INCONSITENCY

Alarm	Attributes	Applicable major release
Name: WmmSYS_CPM_USERDATA_ INCONSITENCY (4342) Type: mmeAlarm Package: Itemme.WmmSYS_CPM_USERDATA_ INCONSITENCY Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A possible CPM user data inconsistency problem has been detected on the MI.		
Remedial action: Login to active MI as root execute 'mividstat -a'\nMake sure CPM is enabled and Connection Health Check is Yes. If not, please refer to CDOC 270-702-015 section 'CPM and RBAC' to enable CPM.\nIf CPM status is OK and there is such alarm. Please contact your Nokia support representative for further support.\nOnce the issue is resolved, this alarm should be cleared manually from the MI GUI.		

Table 24-284 WmmSYS_CPM_USERDATA_RESTORED

Alarm	Attributes	Applicable major release
Name: WmmSYS_CPM_USERDATA_RESTORED (4343) Type: mmeAlarm Package: ltemme.WmmSYS_CPM_USERDATA_RESTORED Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: CPM audit restore user's data after it finds issue.		
Remedial action: Login to active MI as root execute 'mividstat -a'\nMake sure CPM is enabled and Connection Health Check is Yes. If not, please refer to CDOC 270-702-015 section 'CPM and RBAC' to enable CPM.\nIf CPM status is OK and there is such alarm. Please contact your Nokia support representative for further support.\nOnce the issue is resolved, this alarm should be cleared manually from the MI GUI.		

Table 24-285 WmmSYS_EventQueueCapacity

Alarm	Attributes	Applicable major release
Name: WmmSYS_EventQueueCapacity (4345) Type: mmeAlarm Package: ltemme.WmmSYS_EventQueueCapacity Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The MI event queue is nearing or has exceeded it's capacity.		
Remedial action: If the problem persists, contact your Nokia support representative.		

Table 24-286 WmmSYS_ICMPFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_ICMPFailure (4346) Type: mmeAlarm Package: ltemme.WmmSYS_ICMPFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-286 WmmSYS_ICMPFailure (continued)

Alarm	Attributes	Applicable major release
Description: The MI was unable to communicate to a host via its IP interface.		
Remedial action: Verify that the ethernet cable is connected and in working order.\nVerify that the routers/switches are configured correctly.\nIf the problem persists over several polling cycles, contact your Nokia support representative.		

Table 24-287 WmmSYS_IPsecConfig

Alarm	Attributes	Applicable major release
Name: WmmSYS_IPsecConfig (4347) Type: mmeAlarm Package: Itemme.WmmSYS_IPsecConfig Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Missing or obsolete SNMP Trap subnets found in the IPsec configuration file on the MI-Agent.		
Remedial action: A change to the IPsec configuration is needed. Please refer to the procedure described in the section titled 'To configure IPsec SNMP trap entries' in the '5400 Linux Control Platform, Security Management' guide for the ATCA platform, or in the 'Control Platform 1800 OAMP' guide for the CPSB platform.		

Table 24-288 WmmSYS_LinkDown

Alarm	Attributes	Applicable major release
Name: WmmSYS_LinkDown (4348) Type: mmeAlarm Package: Itemme.WmmSYS_LinkDown Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A linkDown alarm signifies that the operational status for one of the communication links is about to enter the down state. The name/index of the interface is identified in the specificProblem of the alarm.		
Remedial action: Verify the cabling.\nVerify the far-end of the link.		

Table 24-289 WmmSYS_NotifyDisabled

Alarm	Attributes	Applicable major release
Name: WmmSYS_NotifyDisabled (4349) Type: mmeAlarm Package: ltemme.WmmSYS_NotifyDisabled Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when a user login is temporarily disabled, yet the user during this period attempts to login with the correct userid and password. User Intervention by a Security Administrator is not required when an user is temporarily disabled as long as no more logins are attempted within fifteen minutes interval. If a user becomes locked then an additional alarm (SYS_NotifyLocked) will be generated thus Security Administrator intervention will be required.		
Remedial action: Contact the user of this userid to determine if they are aware of these attempts to log on to the system using this userid.\nDetermine whether any security violations occurred and report accordingly. Manually clear this alarm from the MI Alarm Browser.		

Table 24-290 WmmSYS_NotifyLocked

Alarm	Attributes	Applicable major release
Name: WmmSYS_NotifyLocked (4350) Type: mmeAlarm Package: ltemme.WmmSYS_NotifyLocked Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when a user is locked out from being able to Log in due to repeated consecutive login failures. User Intervention by a Security Administrator is required to unlock the account.		
Remedial action: Contact the user of this userid to determine if they are aware of these attempts to log on to the system using this userid.\nDetermine whether any security violations occurred and report accordingly Log onto NavisID GUI and unlock this user's account if appropriate. Manually clear this alarm from the MI Alarm Browser.		

Table 24-291 WmmSYS_RADIUS_TO_LDAP_FAILURE

Alarm	Attributes	Applicable major release
Name: WmmSYS_RADIUS_TO_LDAP_FAILURE (4351) Type: mmeAlarm Package: Itemme.WmmSYS_RADIUS_TO_LDAP_FAILURE Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when RADIUS fails to connect to LDAP during user authentication attempt		
Remedial action: This Alarm clears automatically when the fault condition is no longer present.\nLog in to active MI (ATCA) as root execute 'mividstat -a'\nMake sure that Radius/LDAP Connection Health Check is Yes\nCheck the /var/log/auth.log for detailed information. You may also use the Security and Audit Trail Log Viewer on the MI-agent GUI to view this log.		

Table 24-292 WmmSYS_ROOT_ACCESS_DENIED

Alarm	Attributes	Applicable major release
Name: WmmSYS_ROOT_ACCESS_DENIED (4352) Type: mmeAlarm Package: Itemme.WmmSYS_ROOT_ACCESS_DENIED Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when a user makes three attempts within a 30 minute period to log onto the LCP hosts as root userid from a restricted domain. This alarm must be manually cleared		
Remedial action: This Alarm should be cleared manually.\nNeed to find out where the user is trying to log in from to further verify whether this is a legitimate user.\nCheck the /var/log/auth.log for detailed information. You may also use the Security and Audit Trail Log Viewer on the MI-agent GUI to view this log.		

Table 24-293 WmmSYS_ROOT_FTP_VIOLATION

Alarm	Attributes	Applicable major release
Name: WmmSYS_ROOT_FTP_VIOLATION (4353) Type: mmeAlarm Package: ltemme.WmmSYS_ROOT_FTP_VIOLATION Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when an user try to login the system three times as root with wrong password in less 30 seconds. This alarm must be manually cleared.		
Remedial action: Need to find out where is the user attempted to log in.\nCheck the /var/log/auth.log for detailed information.		

Table 24-294 WmmSYS_ROOT_LOGIN_VIOLATION

Alarm	Attributes	Applicable major release
Name: WmmSYS_ROOT_LOGIN_VIOLATION (4354) Type: mmeAlarm Package: ltemme.WmmSYS_ROOT_LOGIN_VIOLATION Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when an user try to login the system three times as root with wrong password in less 30 seconds. This alarm must be manually cleared.		
Remedial action: Need to find out where is the user attempted to log in.\nCheck the /var/log/auth.log for detailed information.		

Table 24-295 WmmSYS_ROOT_SSH_LOGIN_VIOLATION

Alarm	Attributes	Applicable major release
Name: WmmSYS_ROOT_SSH_LOGIN_VIOLATION (4355) Type: mmeAlarm Package: ltemme.WmmSYS_ROOT_SSH_LOGIN_VIOLATION Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0

Table 24-295 WmmSYS_ROOT_SSH_LOGIN_VIOLATION (continued)

Alarm	Attributes	Applicable major release
Description: This alarm occurs when a user unsuccessfully attempts to ssh as root user onto the LCP host three times within 30 minutes. NOTE: If Disable Root SSH External Access feature is enabled, any external ssh as root attempt to the LCP host will be rejected and treated as a login failure. This alarm must be manually cleared.		
Remedial action: Need to check the /var/log/auth.log to identify the IP of the originating ssh request and attempt to identify the user attempting access the LCP host as root userid.\nCheck the /var/log/auth.log for detailed information.\nThe alarm must be manually cleared on the MI GUI.		

Table 24-296 WmmSYS_SetupAAAFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_SetupAAAFailure (4361) Type: mmeAlarm Package: ltemme.WmmSYS_SetupAAAFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: A possible CPM configuration problem has been detected on the MI.		
Remedial action: Login to active MI as root execute 'mividstat -a'\nMake sure CPM is enabled and Connection Health Check is Yes. If not, please refer to CDOC 270-702-015 section 'CPM and RBAC' to enable CPM.\nCheck all the diskful and diskless blades are in service.\nPlease contact your Nokia support representative for further support.\nOnce the issue is resolved, this alarm should be cleared manually from the MI GUI.		

Table 24-297 WmmSYS_SNETrapOverload

Alarm	Attributes	Applicable major release
Name: WmmSYS_SNETrapOverload (4356) Type: mmeAlarm Package: ltemme.WmmSYS_SNETrapOverload Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The SNMP trap rate threshold for a particular SNE to the MI-Agent has been exceeded.		
Remedial action: Verify the sanity of the SNE to determine what is causing it to send excessive SNMP traps to the MI-Agent.\nAs the cause for excessive traps can vary by instance, use standard fault detection techniques such as viewing alarms and/or network events at the MI-Agent, visual inspection of the SNE for external alarms and/or loose cables, and running diagnostic test to assist in determining the cause.		

Table 24-298 WmmSYS_SNMPAuthenticationFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_SNMPAuthenticationFailure (4357) Type: mmeAlarm Package: ltemme.WmmSYS_ SNMPAuthenticationFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: Signifies that an SNE managed by the MI is the addressee of an improperly authenticated network protocol message. SNMP community name and client authentication failures cause the Element Manager to generate this trap.		
Remedial action: Verify that the individual trying to access the system is a legitimate user, and that the SNMP community strings are set correctly. This alarm may be disabled by turning off the SNMP authentication traps on the SNE (providing the SNE supports this capability).		

Table 24-299 WmmSYS_SNMPFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_SNMPFailure (4358) Type: mmeAlarm Package: ltemme.WmmSYS_SNMPFailure Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The MI was unable to communicate to a host via its SNMP interface.		
Remedial action: Verify that the ethernet cable is connected and in working order.\nVerify that the SNE may be ICMP-pinged over the same interface to determine whether it is an SNMP problem or a more general IP problem.\nIf the problem is an IP problem, verify that the routers/switches are configured correctly.\nIf the problem is only an SNMP problem and persists over several polling cycles, contact your Nokia support representative.		

Table 24-300 WmmSYS_SU_TO_ROOT_FAILURE

Alarm	Attributes	Applicable major release
Name: WmmSYS_SU_TO_ROOT_FAILURE (4359) Type: mmeAlarm Package: ltemme.WmmSYS_SU_TO_ROOT_ FAILURE Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm occurs when a user makes three failed attempts within a 30 minute period to su to become root userid. This alarm will occur if you entered the wrong password for root three times during the 30 minute interval when attempting to su to root userid.		
Remedial action: This Alarm should be cleared manually.\nNeed to find out where the user is trying to log in from to further verify whether this is a legitimate user. Need to check the user's CLI shell history to investigate for possible suspicious activity.\nCheck the /var/log/auth.log for detailed access information. Check the /var/log/bash.log to investigate the user's cli activity. You may also use the Security and Audit Trail Log Viewer on the MI-agent GUI to view these logs.		

Table 24-301 WmmSYS_SYSTEMTrapOverload

Alarm	Attributes	Applicable major release
Name: WmmSYS_SYSTEMTrapOverload (4360) Type: mmeAlarm Package: ltemme.WmmSYS_SYSTEMTrapOverload Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The SNMP trap rate threshold for a collection of SNEs to the MI-Agent has been exceeded.		
Remedial action: Verify the sanity of all SNEs in the system to determine which ones are sending excessive SNMP traps to the MI-Agent.\nAs the cause for excessive traps can vary by instance, use standard fault detection techniques such as viewing alarms and/or network events at the MI-Agent, visual inspection of the SNE for external alarms and/or loose cables, and running diagnostic test to assist in determining the cause.		

Table 24-302 WmmSYS_TestAlarm

Alarm	Attributes	Applicable major release
Name: WmmSYS_TestAlarm (4362) Type: mmeAlarm Package: ltemme.WmmSYS_TestAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: This alarm is for testing only. There is no problem being reported. It is used to test the alarm handling functionality on the MI, from creation of an alarm on the MI to forwarding out through the MI's northbound interface. This alarm should be manually cleared when testing is completed.		
Remedial action: There is no recovery needed, as this is just a test alarm. The alarm can be cleared manually on the MI GUI, or by running mi_testalarm -s Clear on the active MI.		

Table 24-303 WmmSYS_ThresholdCrossed

Alarm	Attributes	Applicable major release
Name: WmmSYS_ThresholdCrossed (4363) Type: mmeAlarm Package: ltemme.WmmSYS_ThresholdCrossed Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The measurement data is not meeting the specified performance thresholds and the measurement data has reported errors that may indicate loss or degradation of functionality or capacity.		
Remedial action: Pay attention to the measurement data for which the alarm is reported.\nStudy the state of the system to decide on a course of action.		

Table 24-304 WmmSYS_UndiscoveredObject

Alarm	Attributes	Applicable major release
Name: WmmSYS_UndiscoveredObject (4364) Type: mmeAlarm Package: Itemme.WmmSYS_UndiscoveredObject Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: One or more undiscovered objects have been detected on the MI.		
Remedial action: On the MI GUI, run Tools->Global Discovery. If this does not clear the alarm, run the following command on the active MI host: If specificProblem is MissingSNE:<ip address>: mi_audit -a disc_sne If specificProblem is MissingHardware: mi_audit -a disc_hw If specificProblem is MissingServices: mi_audit -a disc_services If specificProblem is MissingHosts: mi_audit -a disc_hosts contact your Nokia support representative with the alarm details and the output of the mi_audit cmd.		

Table 24-305 WmmSYS_WriteAAAFailure

Alarm	Attributes	Applicable major release
Name: WmmSYS_WriteAAAFailure (4365) Type: mmeAlarm Package: Itemme.WmmSYS_WriteAAAFailure Raised on class: Itemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mmeUnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: CPM tools failed to create scripts that are used for pump data into blades.		
Remedial action: Login to active MI (ATCA) as root execute 'mividstat -a'\nMake sure CPM is enabled and Connection Health Check is Yes. If not, please refer to CDOC 270-702-015 section 'CPM and RBAC' to enable CPM.\nCheck all the diskful and diskless blades are in service.\nCheck existence and permission(Owner:root, permission:755) for the directory /var/opt/lib/cpm/fg on active MI.\nPlease contact your Nokia support representative for further support.\nOnce the issue is resolved, this alarm should be cleared manually from the MI GUI.		

Table 24-306 WMMUEOccupiedSlotsExceeded

Alarm	Attributes	Applicable major release
Name: WMMUEOccupiedSlotsExceeded (5050) Type: communicationsAlarm Package: ltemme.WMMUEOccupiedSlotsExceeded Raised on class: ltemme.MmeInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ThresholdExceeded	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 9.11.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when the number of WMM UE Occupied Slots exceeds the threshold that has been set by the operator.		
Raising condition: (('WMM UE Occupied Slots Threshold' NOT EQUAL '0L') AND ('WMM UE Occupied Slots' > 'WMM UE Occupied Slots Threshold'))		
Remedial action: Informational - no corrective action required.		

Table 24-307 WmmUnknownAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownAlarm (4366) Type: mmeAlarm Package: ltemme.WmmUnknownAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: alarmIndicationSignal	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-308 WmmUnknownCommunicationsAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownCommunicationsAlarm (4367) Type: communicationsAlarm Package: ltemme. WmmUnknownCommunicationsAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown communications alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-309 WmmUnknownEnvironmentalAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownEnvironmentalAlarm (4368) Type: environmentalAlarm Package: ltemme.WmmUnknownEnvironmentalAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown environmental alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-310 WmmUnknownEquipmentAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownEquipmentAlarm (4369) Type: equipmentAlarm Package: ltemme.WmmUnknownEquipmentAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown equipment alarm is received from the WMM system.		

Table 24-310 WmmUnknownEquipmentAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-311 WmmUnknownIntegrityViolationAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownIntegrityViolationAlarm (4370) Type: integrityViolationAlarm Package: ltemme. WmmUnknownIntegrityViolationAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown integrity violation alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-312 WmmUnknownOperationalViolationAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownOperationalViolationAlarm (4371) Type: operationalViolationAlarm Package: ltemme. WmmUnknownOperationalViolationAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown operational alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-313 WmmUnknownPhysicalViolationAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownPhysicalViolationAlarm (4372) Type: physicalViolationAlarm Package: ltemme.WmmUnknownPhysicalViolationAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown physical violation alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-314 WmmUnknownProcessingErrorAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownProcessingErrorAlarm (4373) Type: processingErrorAlarm Package: ltemme.WmmUnknownProcessingErrorAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown processing error alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-315 WmmUnknownQualityOfServiceAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownQualityOfServiceAlarm (4374) Type: qualityOfServiceAlarm Package: ltemme.WmmUnknownQualityOfServiceAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown quality of service alarm is received from the WMM system.		

Table 24-315 WmmUnknownQualityOfServiceAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-316 WmmUnknownSecurityServiceOrMechanismViolationAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownSecurityServiceOr-MechanismViolationAlarm (4375) Type: securityServiceOrMechanismViolationAlarm Package: ltemme.WmmUnknownSecurityServiceOr-MechanismViolationAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown mechanical violation alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 24-317 WmmUnknownTimeDomainViolationAlarm

Alarm	Attributes	Applicable major release
Name: WmmUnknownTimeDomainViolationAlarm (4376) Type: timeDomainViolationAlarm Package: ltemme.WmmUnknownTimeDomainViolationAlarm Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 8.0.0 • 8.1.0 • 9.0.0 • 9.1.0 • 10.0.0 • 10.1.0
Description: The alarm is raised when an unknown time domain violation alarm is received from the WMM system.		
Remedial action: Obtain the native WMM alarm name from the additional text field. Open the 9471 WMM MI GUI and locate the corresponding WMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

25 9500 MPR

25.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 25-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 25-2 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 25-3 AesFipsFail

Alarm	Attributes	Applicable major release
Name: AesFipsFail (11279) Type: equipmentAlarm Package: equipment.AesFipsFail Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AesFipsFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when AES FIPS Failure occurs.		
Remedial action: Please refer to node Troubleshooting guide for detailed steps for corrective action.		

Table 25-4 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 25-5 AtpcLoopProblem (equipment)

Alarm	Attributes	Applicable major release
Name: AtpcLoopProblem (1142) Type: communicationsAlarm Package: equipment.AtpcLoopProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcLoopProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a local transmitter was operating continuously at full power for 5-minutes, and the transmitter power is reduced to its minimum power setting.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-6 AtpcLoopProblem (radioequipment)

Alarm	Attributes	Applicable major release
Name: AtpcLoopProblem (1142) Type: communicationsAlarm Package: radioequipment.AtpcLoopProblem Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcLoopProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a local transmitter was operating continuously at full power for 5-minutes, and the transmitter power is reduced to its minimum power setting.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-7 ATPCTimeout (equipment)

Alarm	Attributes	Applicable major release
Name: ATPCTimeout (3939) Type: communicationsAlarm Package: equipment.ATPCTimeout Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcTimeout	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a the ATPC timeout defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-8 ATPCTimeout (radioequipment)

Alarm	Attributes	Applicable major release
Name: ATPCTimeout (3939) Type: communicationsAlarm Package: radioequipment.ATPCTimeout Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcTimeout	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a the ATPC timeout defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-9 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 25-10 BandwidthDegradeForProtectionSwitch

Alarm	Attributes	Applicable major release
Name: BandwidthDegradeForProtectionSwitch (4414) Type: equipmentAlarm Package: ethring. BandwidthDegradeForProtectionSwitch Raised on class: ethring.Element	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bandwidthDegradeERP	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised on Element instance for 9500 when there are two instance per Radio Component (topology) and when one of the instance is enabled.		
Remedial action: Operator has Unconfigure the protection on ERPS instance.		

Table 25-11 BandwidthOverFlow (radioequipment)

Alarm	Attributes	Applicable major release
Name: BandwidthOverFlow (1143) Type: communicationsAlarm Package: radioequipment.BandwidthOverFlow Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bandwidthOverFlow	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a MPT is on-line and the cross-connections occupation overcomes the MPT net capacity bandwidth.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-12 BandwidthOverFlow (equipment)

Alarm	Attributes	Applicable major release
Name: BandwidthOverFlow (1143) Type: communicationsAlarm Package: equipment.BandwidthOverFlow Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bandwidthOverFlow	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a MPT is on-line and the cross-connections occupation overcomes the MPT net capacity bandwidth.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-13 BatteryFail (mpr)

Alarm	Attributes	Applicable major release
Name: BatteryFail (616) Type: equipmentAlarm Package: mpr.BatteryFail Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: batteryFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the battery fails or is missing.		
Remedial action: The battery on the subrack element should be replaced or re-installed.		

Table 25-14 BerLineSignalDegradation

Alarm	Attributes	Applicable major release
Name: BerLineSignalDegradation (88) Type: communicationsAlarm Package: sonetequipment.BerLineSignalDegradation Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalDegradation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sd alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Degradation') AND ('Report Alarms'anyBit'BER Line Signal Degradation')))		
Remedial action: Informational only.		

Table 25-15 BerLineSignalFailure

Alarm	Attributes	Applicable major release
Name: BerLineSignalFailure (89) Type: communicationsAlarm Package: sonetequipment.BerLineSignalFailure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: berLineSignalFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a line signal degradation BER error. The alarm corresponds to the lb2er-sf alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'BER Line Signal Failure') AND ('Report Alarms'anyBit'BER Line Signal Failure')))		
Remedial action: Informational only.		

Table 25-16 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 25-17 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 25-18 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 25-19 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 25-20 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 25-21 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 25-22 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 25-23 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 25-24 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 25-25 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 25-26 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 25-27 CableLOS (radioequipment)

Alarm	Attributes	Applicable major release
Name: CableLOS (678) Type: communicationsAlarm Package: radioequipment.CableLOS Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cableLOS	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a cable LOS event.		
Remedial action: The alarm is raised when an MSS detects a cable LOS event. Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-28 CableLOS (equipment)

Alarm	Attributes	Applicable major release
Name: CableLOS (678) Type: communicationsAlarm Package: equipment.CableLOS Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cableLOS	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a cable LOS event.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-29 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 25-30 ClockFailure

Alarm	Attributes	Applicable major release
Name: ClockFailure (1162) Type: communicationsAlarm Package: equipment.ClockFailure Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: clockFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT radio clock failure occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-31 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 25-32 CombinerLossOfAlignment (equipment)

Alarm	Attributes	Applicable major release
Name: CombinerLossOfAlignment (5604) Type: equipmentAlarm Package: equipment.CombinerLossOfAlignment Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CombinerLossOfAlignment	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is no alignment between Main and Diversity signal.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-33 CombinerLossOfAlignment (mpr)

Alarm	Attributes	Applicable major release
Name: CombinerLossOfAlignment (5604) Type: equipmentAlarm Package: mpr.CombinerLossOfAlignment Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CombinerLossOfAlignment	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is no alignment between Main and Diversity signal.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-34 CommonLOS

Alarm	Attributes	Applicable major release
Name: CommonLOS (3621) Type: equipmentAlarm Package: equipment.CommonLOS Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: commonLOS	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a radio interface CLA detects a loss of signal.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-35 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 25-36 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 25-37 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 25-38 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 25-39 CrossconnectDown

Alarm	Attributes	Applicable major release
Name: CrossconnectDown (744) Type: CrossconnectAlarm Package: mpr.CrossconnectDown Raised on class: mpr.Crossconnect	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crossconnectDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Operational State of an L2 or L3 interface is Down, and the Administrative State of the associated site is Up. The alarm is not raised against an L2 access interface that is in the MC ring standby state.		
Raising condition: ('xcRowStatus' NOT EQUAL 'Active')		
Clearing condition: ('xcRowStatus' EQUAL 'Active')		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-40 CrossConnectionFail (equipment)

Alarm	Attributes	Applicable major release
Name: CrossConnectionFail (679) Type: communicationsAlarm Package: equipment.CrossConnectionFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crossConnectionFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS TDM cross-connection fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-41 CrossConnectionFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: CrossConnectionFail (679) Type: communicationsAlarm Package: radioequipment.CrossConnectionFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crossConnectionFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS TDM cross-connection fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-42 DAD

Alarm	Attributes	Applicable major release
Name: DAD (4416) Type: communicationsAlarm Package: equipment.DAD Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicatedAddressDetected	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is reported when MPR 9500 detects a duplicated IP address.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-43 DemFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: DemFail (680) Type: communicationsAlarm Package: radioequipment.DemFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS demodulation function fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-44 DemFail (equipment)

Alarm	Attributes	Applicable major release
Name: DemFail (680) Type: communicationsAlarm Package: equipment.DemFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS demodulation function fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-45 DemXpicLOS (equipment)

Alarm	Attributes	Applicable major release
Name: DemXpicLOS (3622) Type: equipmentAlarm Package: equipment.DemXpicLOS Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demXpicLos	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a loss of signal occurs during XPIC demodulation.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-46 DemXpicLOS (mpr)

Alarm	Attributes	Applicable major release
Name: DemXpicLOS (3622) Type: communicationsAlarm Package: mpr.DemXpicLOS Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demXpicLos	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a loss of signal occurs during XPIC demodulation.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-47 DialogFailure (mpr)

Alarm	Attributes	Applicable major release
Name: DialogFailure (1163) Type: equipmentAlarm Package: mpr.DialogFailure Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dialogFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT has a temporary communication failure.		
Remedial action: The alarm is raised upon temporary loss of communication with MPT. Refer to the 9500 Node Maintenance manual for remedial action information		

Table 25-48 DialogFailure (equipment)

Alarm	Attributes	Applicable major release
Name: DialogFailure (1163) Type: equipmentAlarm Package: equipment.DialogFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dialogFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT has a temporary communication failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-49 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 25-50 DS1E1AlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: DS1E1AlarmIndicationSignal (112) Type: communicationsAlarm Package: tdmequipment.DS1E1AlarmIndicationSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: alarmIndicationSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an AIS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Alarm Indication Signal') AND ('Report Alarms'anyBit'Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 25-51 DS1E1Looped

Alarm	Attributes	Applicable major release
Name: DS1E1Looped (126) Type: communicationsAlarm Package: tdmequipment.DS1E1Looped Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: farEndLoopback	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a remote loopback alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Far end wants the near end to loopback') AND ('Report Alarms'anyBit'Far end wants the near end to loopback')))		
Remedial action: Informational only.		

Table 25-52 DS1E1LossOfSignal

Alarm	Attributes	Applicable major release
Name: DS1E1LossOfSignal (124) Type: communicationsAlarm Package: tdmequipment.DS1E1LossOfSignal Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an LOS alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Signal') AND ('Report Alarms'anyBit'Loss of Signal')))		
Remedial action: Informational only.		

Table 25-53 DS1E1OutOfFrame

Alarm	Attributes	Applicable major release
Name: DS1E1OutOfFrame (125) Type: communicationsAlarm Package: tdmequipment.DS1E1OutOfFrame Raised on class: tdmequipment.DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfFrame	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an OOF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Out Of Frame') AND ('Report Alarms'anyBit'Out Of Frame')))		
Remedial action: Informational only.		

Table 25-54 DS1E1ResourceAvailabilityIndicator

Alarm	Attributes	Applicable major release
Name: DS1E1ResourceAvailabilityIndicator (114) Type: communicationsAlarm Package: tdmequipment. DS1E1ResourceAvailabilityIndicator Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAvailabilityIndicator	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an RAI alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Resource Availability Indicator') AND ('Report Alarms'anyBit'Resource Availability Indicator')))		
Remedial action: Informational only.		

Table 25-55 DS1E1SignalDegradation

Alarm	Attributes	Applicable major release
Name: DS1E1SignalDegradation (500) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalDegradation Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalDegradation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SD alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Degradation') AND ('Report Alarms'anyBit'Signal Degradation')))		
Remedial action: Informational only.		

Table 25-56 DS1E1SignalFailure

Alarm	Attributes	Applicable major release
Name: DS1E1SignalFailure (501) Type: communicationsAlarm Package: tdmequipment.DS1E1SignalFailure Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has an SF alarm condition.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: Informational only.		

Table 25-57 EarlyWarning (radioequipment)

Alarm	Attributes	Applicable major release
Name: EarlyWarning (681) Type: communicationsAlarm Package: radioequipment.EarlyWarning Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: earlyWarning	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects an early warning event.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-58 EarlyWarning (equipment)

Alarm	Attributes	Applicable major release
Name: EarlyWarning (681) Type: communicationsAlarm Package: equipment.EarlyWarning Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: earlyWarning	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects an early warning event.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-59 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 25-60 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 25-61 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 25-62 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 25-63 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 25-64 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 25-65 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 25-66 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 25-67 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 25-68 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 25-69 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 25-70 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 25-71 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 25-72 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 25-73 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 25-74 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 25-75 ExcessiveEnvironmentTemparature (equipment)

Alarm	Attributes	Applicable major release
Name: ExcessiveEnvironmentTemparature (1118) Type: environmentalAlarm Package: equipment.ExcessiveEnvironmentTemparature Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: excessiveEnvironmentTemp	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when MPT is overheated.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-76 ExcessiveEnvironmentTemparature (mpr)

Alarm	Attributes	Applicable major release
Name: ExcessiveEnvironmentTemparature (1118) Type: communicationsAlarm Package: mpr.ExcessiveEnvironmentTemparature Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: excessiveEnvironmentTemp	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when MPT is overheated.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-77 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 25-78 FanCommunicationProblem

Alarm	Attributes	Applicable major release
Name: FanCommunicationProblem (5424) Type: communicationsAlarm Package: mpr.FanCommunicationProblem Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanCommunicationProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a communication problem with fan is detected.		
Remedial action: The alarm is raised when FAN communication Problem is detected on the subrack. Refer 9500 Node Maintenance manual for remedial action information		

Table 25-79 FanFail

Alarm	Attributes	Applicable major release
Name: FanFail (5609) Type: equipmentAlarm Package: equipment.FanFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is fan fail for MPTHLC.		
Remedial action: The alarm is raised when MPTHLC fan fails. Refer 9500 Node Maintenance manual for remedial action information.		

Table 25-80 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 25-81 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 25-82 FirmwareDownloadOnGoing (mpr)

Alarm	Attributes	Applicable major release
Name: FirmwareDownloadOnGoing (626) Type: equipmentAlarm Package: mpr.FirmwareDownloadOnGoing Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: firmwareDownloadOnGoing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a firmware download is in progress.		
Remedial action: Informational - Firmware for the equipment is downloading.		

Table 25-83 FlashCardFailure

Alarm	Attributes	Applicable major release
Name: FlashCardFailure (8161) Type: equipmentAlarm Package: equipment.FlashCardFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: flashCardFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is Flash card failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-84 FlashCardRealignmentInProgress

Alarm	Attributes	Applicable major release
Name: FlashCardRealignmentInProgress (8162) Type: equipmentAlarm Package: equipment. FlashCardRealignmentInProgress Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: flashCardRealignmentIn-Progress	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when MPR Flash card realignment is in progress.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-85 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 25-86 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 25-87 HighBER (radioequipment)

Alarm	Attributes	Applicable major release
Name: HighBER (682) Type: communicationsAlarm Package: radioequipment.HighBER Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: highBER	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a high BER.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-88 HouseKeeping (mpr)

Alarm	Attributes	Applicable major release
Name: HouseKeeping (1165) Type: equipmentAlarm Package: mpr.HouseKeeping Raised on class: mpr.AbstractMprAux	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HouseKeeping	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: Defect detected by an house-keeping interface on AUX card.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-89 HouseKeeping (equipment)

Alarm	Attributes	Applicable major release
Name: HouseKeeping (1165) Type: equipmentAlarm Package: equipment.HouseKeeping Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: houseKeeping	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a HouseKeeping trap is received.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-90 IncompatibleFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleFrequency (683) Type: communicationsAlarm Package: equipment.IncompatibleFrequency Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleFrequency	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a provisioned MSS frequency is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-91 IncompatibleFrequency (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleFrequency (683) Type: communicationsAlarm Package: radioequipment.IncompatibleFrequency Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleFrequency	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a provisioned MSS frequency is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-92 IncompatibleModulation (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulation (4417) Type: communicationsAlarm Package: radioequipment.IncompatibleModulation Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an incompatibility of the modulation value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-93 IncompatibleModulation (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulation (4417) Type: communicationsAlarm Package: equipment.IncompatibleModulation Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an incompatibility of the modulation value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-94 IncompatibleModulationParam (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm Package: equipment.IncompatibleModulationParam Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the configured modulation parameters are not supported by MPT (or) when XPIC is configured on an MPT that does not allow XPIC capability.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-95 IncompatibleModulationParam (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm Package: radioequipment. IncompatibleModulationParam Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the configured modulation parameters are not supported by MPT (or) when XPIC is configured on an MPT that does not allow XPIC capability.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-96 IncompatiblePower (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePower (3940) Type: communicationsAlarm Package: equipment.IncompatiblePower Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePower	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of the power value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-97 IncompatiblePower (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePower (3940) Type: communicationsAlarm Package: radioequipment.IncompatiblePower Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePower	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of the power value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-98 IncompatibleProtection (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleProtection (4824) Type: equipmentAlarm Package: equipment.IncompatibleProtection Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleProtection	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised in case of hardware incompatibility for 1+1 radio configuration i.e. MPT-HCv2 without RPS or XPIC equipped.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-99 IncompatiblePTX (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePTX (684) Type: communicationsAlarm Package: radioequipment.IncompatiblePTX Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePTX	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS transmit power is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-100 IncompatiblePTX (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePTX (684) Type: communicationsAlarm Package: equipment.IncompatiblePTX Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePTX	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS transmit power is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-101 IncompatibleShifter (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleShifter (685) Type: communicationsAlarm Package: radioequipment.IncompatibleShifter Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleShifter	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS shifter parameters are incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-102 IncompatibleShifter (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleShifter (685) Type: communicationsAlarm Package: equipment.IncompatibleShifter Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleShifter	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS shifter parameters are incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-103 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 25-104 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 25-105 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 25-106 InternalCommunicationProblem (equipment)

Alarm	Attributes	Applicable major release
Name: InternalCommunicationProblem (627) Type: equipmentAlarm Package: equipment.InternalCommunicationProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: internalCommunicationProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an ODU is unresponsive.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-107 InternalCommunicationProblem (mpr)

Alarm	Attributes	Applicable major release
Name: InternalCommunicationProblem (627) Type: equipmentAlarm Package: mpr.InternalCommunicationProblem Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: internalCommunicationProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPTHLv2 is unresponsive.		
Remedial action: The alarm is raised when there is a loss of communication with MPT. Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-108 KeyUnavailable

Alarm	Attributes	Applicable major release
Name: KeyUnavailable (11291) Type: communicationsAlarm Package: equipment.KeyUnavailable Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: KeyUnavailable	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when Key Unavailable is there for secure certified mode.		
Remedial action: Please refer to node Troubleshooting guide for detailed steps for corrective action.		

Table 25-109 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 25-110 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 25-111 LagPortDown

Alarm	Attributes	Applicable major release
Name: LagPortDown (10275) Type: communicationsAlarm Package: equipment.LagPortDown Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagPortDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the lag port is down.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-112 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 25-113 LineAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: LineAlarmIndicationSignal (84) Type: communicationsAlarm Package: sonetequipment.LineAlarmIndicationSignal Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineAlarmIndicationSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports an LAIS error. The alarm corresponds to the lais alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Alarm Indication Signal') AND ('Report Alarms'anyBit'Line Alarm Indication Signal')))		
Remedial action: Informational only.		

Table 25-114 LineErrorCondition

Alarm	Attributes	Applicable major release
Name: LineErrorCondition (94) Type: communicationsAlarm Package: sonetequipment.LineErrorCondition Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineErrorCondition	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a line error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Error Condition') AND ('Report Alarms'anyBit'Line Error Condition')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 25-115 LineRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: LineRemoteDefectIndication (85) Type: communicationsAlarm Package: sonetequipment.LineRemoteDefectIndication Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lineRemoteDefectIndication	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a line remote defect indication error caused by an LOF, LOC, or LOS condition. The alarm corresponds to the lrdi alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Line Remote Defect Indication') AND ('Report Alarms'anyBit'Line Remote Defect Indication')))		
Remedial action: Informational only.		

Table 25-116 LinkCle

Alarm	Attributes	Applicable major release
Name: LinkCle (8437) Type: communicationsAlarm Package: equipment.LinkCle Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkcle	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when at least one of the Critical Link Event flags is received.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-117 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 25-118 LinkIdentifierMismatch (radioequipment)

Alarm	Attributes	Applicable major release
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm Package: radioequipment.LinkIdentifierMismatch Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkIdentifierMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a link identifier mismatch.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-119 LinkIdentifierMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm Package: equipment.LinkIdentifierMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkIdentifierMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a link identifier mismatch.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-120 LinkOdnc

Alarm	Attributes	Applicable major release
Name: LinkOdnc (8438) Type: communicationsAlarm Package: equipment.LinkOdnc Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkodnc	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when a OAM Discovery is not completed.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-121 LocalAccessRequested

Alarm	Attributes	Applicable major release
Name: LocalAccessRequested (9631) Type: equipmentAlarm Package: mpr.LocalAccessRequested Raised on class: mpr.MprNeProperties	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lacRequested	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Local access is requested by CT		
Raising condition: (('Lac state' EQUAL 'Access Requested'))		
Clearing condition: ('Lac state' NOT EQUAL 'Access Requested')		
Remedial action: Alarm is raised when CT requests access to NE. Navigate to System settings and grant local access if needed or ignore the request and wait for the timeout to expire for alarm to clear.		

Table 25-122 LoopProblem (equipment)

Alarm	Attributes	Applicable major release
Name: LoopProblem (1145) Type: communicationsAlarm Package: equipment.LoopProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: loopProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a loss of communication command path between far end transmitter and local receiver .		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-123 LoopProblem (radioequipment)

Alarm	Attributes	Applicable major release
Name: LoopProblem (1145) Type: communicationsAlarm Package: radioequipment.LoopProblem Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: loopProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a loss of communication command path between far end transmitter and local receiver .		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-124 LossOfCESoEthFrames

Alarm	Attributes	Applicable major release
Name: LossOfCESoEthFrames (1168) Type: communicationsAlarm Package: equipment.LossOfCESoEthFrames Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfCESoEthFrames	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an Ethernet frame loss is detected on a CES.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-125 LossOfClock (sonetequipment)

Alarm	Attributes	Applicable major release
Name: LossOfClock (83) Type: communicationsAlarm Package: sonetequipment.LossOfClock Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfClock	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports an LOC condition, which causes the NE to set the port Operational State to Down.		
Raising condition: (('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Loss of Clock') AND ('Report Alarms'anyBit'Loss of Clock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 25-126 LossOfFrame (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfFrame (630) Type: communicationsAlarm Package: equipment.LossOfFrame Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfFrame	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an LOF is detected on a port.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-127 LossOfMultiFrame (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfMultiFrame (3930) Type: communicationsAlarm Package: equipment.LossOfMultiFrame Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfMultiFrame	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when a loss of multiple frames occurs on the SDH port.		
Remedial action: This alarm is raised when there is a loss of multiple frames on the SDH port.		

Table 25-128 LossOfProtection

Alarm	Attributes	Applicable major release
Name: LossOfProtection (1169) Type: communicationsAlarm Package: equipment.LossOfProtection Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfProtection	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT radio protection loss occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-129 LossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfSignal (631) Type: communicationsAlarm Package: equipment.LossOfSignal Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a Loss of Signal is detected on a port.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-130 LowInputVoltage

Alarm	Attributes	Applicable major release
Name: LowInputVoltage (9619) Type: environmentalAlarm Package: equipment.LowInputVoltage Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lowInputVoltage	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when Low input voltage is detected.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-131 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 25-132 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 25-133 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 25-134 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 25-135 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		

Table 25-135 NewSsh2ServerKeyDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 25-136 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 25-137 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 25-137 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 25-138 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 25-139 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 25-140 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 25-141 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 25-142 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 25-143 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 25-144 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 25-145 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 25-146 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 25-147 PPPFail

Alarm	Attributes	Applicable major release
Name: PPPFail (632) Type: communicationsAlarm Package: equipment.PPPFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pppFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a PPP IP Fail condition is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-148 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 25-149 ProvisioningMismatch

Alarm	Attributes	Applicable major release
Name: ProvisioningMismatch (634) Type: equipmentAlarm Package: equipment.ProvisioningMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: provisioningMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a license mismatch is detected for provisioned equipment.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-150 PTP1588TCFail

Alarm	Attributes	Applicable major release
Name: PTP1588TCFail (9621) Type: communicationsAlarm Package: equipment.PTP1588TCFail Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ptp1588tcFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when ptp failure is detected.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-151 PTPClockclassDEG

Alarm	Attributes	Applicable major release
Name: PTPClockclassDEG (11511) Type: communicationsAlarm Package: ptp.PTPClockclassDEG Raised on class: ptp.IEEEPTPClock	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPClockclassDEG	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised if PTP clockclass is smaller than the value of the specific threshold.		
Remedial action: Please check if the configured Peer PTP clockclass configuration is correct.		

Table 25-152 PTPPeerDelayRespPkt

Alarm	Attributes	Applicable major release
Name: PTPPeerDelayRespPkt (11512) Type: communicationsAlarm Package: ptp.PTPPeerDelayRespPkt Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerDelayRespPkt	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised if the 1588 Delay_resp packet is not received.		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is correct.		

Table 25-153 PTPPeerLossOfAnnounce

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfAnnounce (3608) Type: communicationsAlarm Package: ptp.PTPPeerLossOfAnnounce Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfAnnounce	Release: • 7.1.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Announce)' state. This indicates that the PTP announce messages are not received from the remote master.		

Table 25-153 PTPPeerLossOfAnnounce (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Master GM Alarms'anyBit'Loss of Announce'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Announce')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 25-154 PTPPeerLossOfSync

Alarm	Attributes	Applicable major release
Name: PTPPeerLossOfSync (3609) Type: communicationsAlarm Package: ptp.PTPPeerLossOfSync Raised on class: ptp.IEEEPTPPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPeerLossOfSync	Release: • 7.1.0
Description: The alarm is raised when the PTP peer is in the 'Packet Timing Signal Fail (Loss Sync)' state. This indicates that the PTP timing messages are not received from the remote master.		
Raising condition: (('Master GM Alarms'anyBit'Loss of Sync'))		
Clearing condition: NOT ((('Master GM Alarms'anyBit'Loss of Sync')))		
Remedial action: Please check if Configured Peer IP address is reachable (ping <Peer Ip>) from the NE and PTP configuration is proper.		

Table 25-155 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 25-156 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 25-157 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 25-158 RadioEncryptionMismatch (radioequipment)

Alarm	Attributes	Applicable major release
Name: RadioEncryptionMismatch (8969) Type: communicationsAlarm Package: radioequipment.RadioEncryptionMismatch Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radioEncryptionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an AES encryption is diffrent between local and remote NE facing on Radio link.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-159 RadioEncryptionMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: RadioEncryptionMismatch (8969) Type: communicationsAlarm Package: equipment.RadioEncryptionMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radioEncryptionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an AES encryption is diffrent between local and remote NE facing on Radio link.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-160 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 25-161 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 25-162 RemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: RemoteDefectIndication (2942) Type: communicationsAlarm Package: equipment.RemoteDefectIndication Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteDefectIndication	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a RDI occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-163 ReplaceableUnitMissing (equipment)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitMissing (635) Type: equipmentAlarm Package: equipment.ReplaceableUnitMissing Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardMissing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device detects that a provisioned card is not physically present.		
Remedial action: Informational - no corrective action required.		

Table 25-164 ReplaceableUnitMissing (mpr)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitMissing (635) Type: equipmentAlarm Package: mpr.ReplaceableUnitMissing Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardMissing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device detects that a provisioned MPT is not physically present.		
Remedial action: The alarm is raised when a device detects that a provisioned card is not physically present.		

Table 25-165 ReplaceableUnitProblem (equipment)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitProblem (636) Type: equipmentAlarm Package: equipment.ReplaceableUnitProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a card fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-166 ReplaceableUnitProblem (mpr)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitProblem (636) Type: equipmentAlarm Package: mpr.ReplaceableUnitProblem Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a card fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-167 ReplaceableUnitTypeMismatch (mpr)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitTypeMismatch (637) Type: equipmentAlarm Package: mpr.ReplaceableUnitTypeMismatch Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a mismatch between the installed equipment type and the expected equipment type.		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 25-168 ReplaceableUnitTypeMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitTypeMismatch (637) Type: equipmentAlarm Package: equipment.ReplaceableUnitTypeMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a mismatch between the installed card type and the expected card type.		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 25-169 RetimingBufferOverFlow

Alarm	Attributes	Applicable major release
Name: RetimingBufferOverFlow (1130) Type: communicationsAlarm Package: equipment.RetimingBufferOverFlow Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufferOverFlow	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an retiming buffer overflow occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-170 RFSwitchFail (equipment)

Alarm	Attributes	Applicable major release
Name: RFSwitchFail (5425) Type: equipmentAlarm Package: equipment.RFSwitchFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rFSwitchFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a RF switch failure is detected.		
Remedial action: The alarm is raised when RF switch failure is detected. Refer 9500 Node Maintenance manual for remedial action information		

Table 25-171 RFSwitchFail (mpr)

Alarm	Attributes	Applicable major release
Name: RFSwitchFail (5425) Type: equipmentAlarm Package: mpr.RFSwitchFail Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rFSwitchFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a RF switch failure is detected.		
Remedial action: The alarm is raised when RF switch failure is detected. Refer 9500 Node Maintenance manual for remedial action information		

Table 25-172 RPSPathFail (equipment)

Alarm	Attributes	Applicable major release
Name: RPSPathFail (8133) Type: equipmentAlarm Package: equipment.RPSPathFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: receiverProtectionFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a receiver protection switchover fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-173 RPSPathFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: RPSPathFail (8133) Type: equipmentAlarm Package: radioequipment.RPSPathFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: receiverProtectionFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a receiver protection switchover fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-174 RxDivMissing

Alarm	Attributes	Applicable major release
Name: RxDivMissing (5646) Type: equipmentAlarm Package: equipment.RxDivMissing Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RxDivMissing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT is attached with combiner enabled and Rx Diversity module is missing.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-175 rxDivMissing

Alarm	Attributes	Applicable major release
Name: rxDivMissing (8372) Type: equipmentAlarm Package: mpr.rxDivMissing Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RxDivMissing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT is attached with combiner enabled and Rx Diversity module is missing.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-176 RxFail (equipment)

Alarm	Attributes	Applicable major release
Name: RxFail (687) Type: communicationsAlarm Package: equipment.RxFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a receive failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-177 RxFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: RxFail (687) Type: communicationsAlarm Package: radioequipment.RxFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a receive failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-178 RxProblem

Alarm	Attributes	Applicable major release
Name: RxProblem (10276) Type: communicationsAlarm Package: equipment.RxProblem Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when Receiver of a lag has problem.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-179 RxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: RxSectionSynchronizationError (93) Type: communicationsAlarm Package: sonetequipment. RxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxSectionSynchronizationError	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'RX Section Synchronization Error') AND ('Report Alarms'anyBit'RX Section Synchronization Error')))		
Remedial action: Check the link status between SONET Port and the source.		

Table 25-180 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 25-181 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 25-182 SecondaryBatteryFail (mpr)

Alarm	Attributes	Applicable major release
Name: SecondaryBatteryFail (3624) Type: equipmentAlarm Package: mpr.SecondaryBatteryFail Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: secondaryBatteryFail	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a secondary battery failure is detected.		
Remedial action: The battery on the subrack element(MPT) should be replaced or re-installed.		

Table 25-183 SectionB1Error

Alarm	Attributes	Applicable major release
Name: SectionB1Error (87) Type: communicationsAlarm Package: sonetequipment.SectionB1Error Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionB1Error	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a section error condition that a remote NE raises because of b1 errors received from the local NE. The alarm corresponds to the lrei alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section B1 Error') AND ('Report Alarms'anyBit'Section B1 Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 25-184 SectionLossOfFrame

Alarm	Attributes	Applicable major release
Name: SectionLossOfFrame (90) Type: communicationsAlarm Package: sonetequipment.SectionLossOfFrame Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfFrame	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a SLOF error. The alarm corresponds to the slof alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Frame') AND ('Report Alarms'anyBit'Section Loss of Frame')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 25-185 SectionLossOfSignal

Alarm	Attributes	Applicable major release
Name: SectionLossOfSignal (91) Type: communicationsAlarm Package: sonetequipment.SectionLossOfSignal Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionLossOfSignal	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a SLOS error. The alarm corresponds to the slos alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section Loss of Signal') AND ('Report Alarms'anyBit'Section Loss of Signal')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected.		

Table 25-186 SectionS1Failure

Alarm	Attributes	Applicable major release
Name: SectionS1Failure (86) Type: communicationsAlarm Package: sonetequipment.SectionS1Failure Raised on class: sonetequipment.SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionS1Failure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports a section synchronization failure. A section synchronization failure occurs when the S1 byte is inconsistent for eight consecutive frames.		
Raising condition: (('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Section S1 Failure') AND ('Report Alarms'anyBit'Section S1 Failure')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 25-187 SectionTraceMismatch

Alarm	Attributes	Applicable major release
Name: SectionTraceMismatch (2943) Type: communicationsAlarm Package: equipment.SectionTraceMismatch Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sectionTraceMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a trace mismatch is detected on a SONET section.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-188 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 25-189 StandbyVersionMismatch (mpr)

Alarm	Attributes	Applicable major release
Name: StandbyVersionMismatch (1174) Type: equipmentAlarm Package: mpr.StandbyVersionMismatch Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: standbyVersionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a standby device software version mismatch is detected.		
Remedial action: This alarm is raised when standby Software version on the MPT does not match the software version on the core. Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-190 StandbyVersionMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: StandbyVersionMismatch (1174) Type: equipmentAlarm Package: equipment.StandbyVersionMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: standbyVersionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a standby device software version mismatch is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-191 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 25-192 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 25-193 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 25-194 SynchronizationSignalFailure

Alarm	Attributes	Applicable major release
Name: SynchronizationSignalFailure (2944) Type: communicationsAlarm Package: equipment.SynchronizationSignalFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: synchronizationSignalFailure	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a synchronization signal failure is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-195 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 25-196 TrafficDown

Alarm	Attributes	Applicable major release
Name: TrafficDown (10277) Type: communicationsAlarm Package: equipment.TrafficDown Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trafficDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when Traffic is down.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-197 TrafficLoss

Alarm	Attributes	Applicable major release
Name: TrafficLoss (10278) Type: communicationsAlarm Package: equipment.TrafficLoss Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trafficLoss	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when a loss is detected in traffic.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-198 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 25-199 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 25-199 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 25-200 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 25-201 TxProblem

Alarm	Attributes	Applicable major release
Name: TxProblem (10279) Type: communicationsAlarm Package: equipment.TxProblem Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txProblem	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when Trasmitter of a lag has problem.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 25-202 TxSectionSynchronizationError

Alarm	Attributes	Applicable major release
Name: TxSectionSynchronizationError (92) Type: communicationsAlarm Package: sonetequipment. TxSectionSynchronizationError Raised on class: sonetequipment. SonetPortMonitorSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txSectionSynchronizationError	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a SONET port reports an SS1F error. The alarm corresponds to the ss1f alarm on an NE.		
Raising condition: (('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'TX Section Synchronization Error') AND ('Report Alarms'anyBit'TX Section Synchronization Error')))		
Remedial action: Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 25-203 UnderlyingResourceUnavailable

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceUnavailable (1131) Type: communicationsAlarm Package: equipment.UnderlyingResourceUnavailable Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an underlying resource is unavailable on an E1, radio, or Ethernet interface.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-204 UnderlyingResourceUnavailableService

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceUnavailableService (1177) Type: communicationsAlarm Package: equipment. UnderlyingResourceUnavailableService Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailableService	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an underlying E1, radio, or Ethernet interface resource service is unavailable.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-205 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 25-206 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 25-207 unsupportedPortUsage

Alarm	Attributes	Applicable major release
Name: unsupportedPortUsage (5184) Type: equipmentAlarm Package: equipment.unsupportedPortUsage Raised on class: equipment.Port	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePortUsage	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised in case unsupported port type is configured		
Remedial action: This alarm indicates unsupported port usage. Port usage configured on the NE is not supported by SAM.		

Table 25-208 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 25-209 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 25-210 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 25-211 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 25-212 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 25-213 VersionMismatch (mpr)

Alarm	Attributes	Applicable major release
Name: VersionMismatch (646) Type: equipmentAlarm Package: mpr.VersionMismatch Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an ODU software version mismatch is detected.		
Remedial action: This alarm is raised when the software version on the MPT does not match the software version on the core. Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-214 VersionMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: VersionMismatch (646) Type: equipmentAlarm Package: equipment.VersionMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an ODU software version mismatch is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 25-215 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 4.1.0 • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

26 9500 MPRe

26.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 26-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 26-2 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		

Table 26-2 adjacencyDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 26-3 AisRx

Alarm	Attributes	Applicable major release
Name: AisRx (1157) Type: communicationsAlarm Package: equipment.AisRx Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aisRx	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a receiver alarm indication signal.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-4 AisTx

Alarm	Attributes	Applicable major release
Name: AisTx (1158) Type: communicationsAlarm Package: equipment.AisTx Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aisTx	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a transmission alarm indication signal.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-5 ATPCTimeout (equipment)

Alarm	Attributes	Applicable major release
Name: ATPCTimeout (3939) Type: communicationsAlarm Package: equipment.ATPCTimeout Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcTimeout	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a the ATPC timeout defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-6 ATPCTimeout (radioequipment)

Alarm	Attributes	Applicable major release
Name: ATPCTimeout (3939) Type: communicationsAlarm Package: radioequipment.ATPCTimeout Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atpcTimeout	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a the ATPC timeout defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-7 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-7 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 26-8 BandwidthOverFlow (radioequipment)

Alarm	Attributes	Applicable major release
Name: BandwidthOverFlow (1143) Type: communicationsAlarm Package: radioequipment.BandwidthOverFlow Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bandwidthOverFlow	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a MPT is on-line and the cross-connections occupation overcomes the MPT net capacity bandwidth.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-9 BandwidthOverFlow (equipment)

Alarm	Attributes	Applicable major release
Name: BandwidthOverFlow (1143) Type: communicationsAlarm Package: equipment.BandwidthOverFlow Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bandwidthOverFlow	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a MPT is on-line and the cross-connections occupation overcomes the MPT net capacity bandwidth.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-10 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 26-11 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 26-12 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 26-13 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 26-14 ClockFailure

Alarm	Attributes	Applicable major release
Name: ClockFailure (1162) Type: communicationsAlarm Package: equipment.ClockFailure Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: clockFailure	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MPT radio clock failure occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-15 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 26-16 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 26-17 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 26-18 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 26-19 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 26-20 CrossConnectionFail (equipment)

Alarm	Attributes	Applicable major release
Name: CrossConnectionFail (679) Type: communicationsAlarm Package: equipment.CrossConnectionFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crossConnectionFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS TDM cross-connection fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-21 CrossConnectionFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: CrossConnectionFail (679) Type: communicationsAlarm Package: radioequipment.CrossConnectionFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crossConnectionFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS TDM cross-connection fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-22 DemFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: DemFail (680) Type: communicationsAlarm Package: radioequipment.DemFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-22 DemFail (radioequipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MSS demodulation function fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-23 DemFail (equipment)

Alarm	Attributes	Applicable major release
Name: DemFail (680) Type: communicationsAlarm Package: equipment.DemFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS demodulation function fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-24 DemXpicLOS (equipment)

Alarm	Attributes	Applicable major release
Name: DemXpicLOS (3622) Type: equipmentAlarm Package: equipment.DemXpicLOS Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demXpicLos	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a loss of signal occurs during XPIC demodulation.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-25 DemXpicLOS (mpr)

Alarm	Attributes	Applicable major release
Name: DemXpicLOS (3622) Type: communicationsAlarm Package: mpr.DemXpicLOS Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: demXpicLos	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a loss of signal occurs during XPIC demodulation.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-26 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 26-27 EarlyWarning (radioequipment)

Alarm	Attributes	Applicable major release
Name: EarlyWarning (681) Type: communicationsAlarm Package: radioequipment.EarlyWarning Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: earlyWarning	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects an early warning event.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-28 EarlyWarning (equipment)

Alarm	Attributes	Applicable major release
Name: EarlyWarning (681) Type: communicationsAlarm Package: equipment.EarlyWarning Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: earlyWarning	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects an early warning event.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-29 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-29 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 26-30 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 26-31 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		

Table 26-31 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 26-32 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 26-33 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 26-34 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 26-35 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 26-36 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 26-37 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 26-38 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 26-39 HighBER (radioequipment)

Alarm	Attributes	Applicable major release
Name: HighBER (682) Type: communicationsAlarm Package: radioequipment.HighBER Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: highBER	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a high BER.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-40 IncompatibleChannelSpacing (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleChannelSpacing (1167) Type: communicationsAlarm Package: radioequipment. IncompatibleChannelSpacing Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleChannelSpacing	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of channel spacing value defect raise.		
Remedial action: The alarm is raised when a incompatibility of channel spacing value defect raise.		

Table 26-41 IncompatibleChannelSpacing (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleChannelSpacing (1167) Type: communicationsAlarm Package: equipment.IncompatibleChannelSpacing Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleChannelSpacing	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of channel spacing value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-42 IncompatibleFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleFrequency (683) Type: communicationsAlarm Package: equipment.IncompatibleFrequency Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleFrequency	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-42 IncompatibleFrequency (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a provisioned MSS frequency is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-43 IncompatibleFrequency (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleFrequency (683) Type: communicationsAlarm Package: radioequipment.IncompatibleFrequency Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleFrequency	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a provisioned MSS frequency is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-44 IncompatibleModulationParam (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm Package: equipment.IncompatibleModulationParam Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the configured modulation parameters are not supported by MPT (or) when XPIC is configured on an MPT that does not allow XPIC capability.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-45 IncompatibleModulationParam (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm Package: radioequipment. IncompatibleModulationParam Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleModulation	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the configured modulation parameters are not supported by MPT (or) when XPIC is configured on an MPT that does not allow XPIC capability.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-46 IncompatiblePower (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePower (3940) Type: communicationsAlarm Package: equipment.IncompatiblePower Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePower	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of the power value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-47 IncompatiblePower (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePower (3940) Type: communicationsAlarm Package: radioequipment.IncompatiblePower Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePower	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a incompatibility of the power value defect raise.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-48 IncompatiblePTX (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePTX (684) Type: communicationsAlarm Package: radioequipment.IncompatiblePTX Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePTX	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS transmit power is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-49 IncompatiblePTX (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatiblePTX (684) Type: communicationsAlarm Package: equipment.IncompatiblePTX Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatiblePTX	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-49 IncompatiblePTX (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the provisioned MSS transmit power is incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-50 IncompatibleShifter (radioequipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleShifter (685) Type: communicationsAlarm Package: radioequipment.IncompatibleShifter Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleShifter	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS shifter parameters are incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-51 IncompatibleShifter (equipment)

Alarm	Attributes	Applicable major release
Name: IncompatibleShifter (685) Type: communicationsAlarm Package: equipment.IncompatibleShifter Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleShifter	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the provisioned MSS shifter parameters are incompatible with the MSS hardware.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-52 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 26-53 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 26-54 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 26-55 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 26-56 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 26-57 LinkIdentifierMismatch (radioequipment)

Alarm	Attributes	Applicable major release
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm Package: radioequipment.LinkIdentifierMismatch Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkIdentifierMismatch	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a link identifier mismatch.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-58 LinkIdentifierMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm Package: equipment.LinkIdentifierMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkIdentifierMismatch	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a link identifier mismatch.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-59 LoopProblem (equipment)

Alarm	Attributes	Applicable major release
Name: LoopProblem (1145) Type: communicationsAlarm Package: equipment.LoopProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: loopProblem	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when there is a loss of communication command path between far end transmitter and local receiver .		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-60 LoopProblem (radioequipment)

Alarm	Attributes	Applicable major release
Name: LoopProblem (1145) Type: communicationsAlarm Package: radioequipment.LoopProblem Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: loopProblem	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-60 LoopProblem (radioequipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when there is a loss of communication command path between far end transmitter and local receiver .		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-61 LossOfFrame (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfFrame (630) Type: communicationsAlarm Package: equipment.LossOfFrame Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfFrame	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an LOF is detected on a port.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-62 LossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: LossOfSignal (631) Type: communicationsAlarm Package: equipment.LossOfSignal Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a Loss of Signal is detected on a port.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-63 LowInputVoltage

Alarm	Attributes	Applicable major release
Name: LowInputVoltage (9619) Type: environmentalAlarm Package: equipment.LowInputVoltage Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lowInputVoltage	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when Low input voltage is detected.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 26-64 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 26-65 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 26-66 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 26-67 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 26-68 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 26-69 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 26-70 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 26-71 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 26-72 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 26-73 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 26-74 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 26-75 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 26-76 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 26-77 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 26-78 PPPFail

Alarm	Attributes	Applicable major release
Name: PPPFail (632) Type: communicationsAlarm Package: equipment.PPPFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pppFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a PPP IP Fail condition is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-79 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 26-80 PTP1588TCFail

Alarm	Attributes	Applicable major release
Name: PTP1588TCFail (9621) Type: communicationsAlarm Package: equipment.PTP1588TCFail Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ptp1588tcFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when ptp failure is detected.		
Remedial action: Please refer MPR documentation for Corrective actions.		

Table 26-81 RadioEncryptionMismatch (radioequipment)

Alarm	Attributes	Applicable major release
Name: RadioEncryptionMismatch (8969) Type: communicationsAlarm Package: radioequipment.RadioEncryptionMismatch Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radioEncryptionMismatch	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an AES encryption is diffrent between local and remote NE facing on Radio link.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-82 RadioEncryptionMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: RadioEncryptionMismatch (8969) Type: communicationsAlarm Package: equipment.RadioEncryptionMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radioEncryptionMismatch	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an AES encryption is diffrent between local and remote NE facing on Radio link.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-83 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-83 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 26-84 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 26-85 RemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: RemoteDefectIndication (2942) Type: communicationsAlarm Package: equipment.RemoteDefectIndication Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteDefectIndication	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-85 RemoteDefectIndication (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a RDI occurs.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-86 ReplaceableUnitMissing (equipment)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitMissing (635) Type: equipmentAlarm Package: equipment.ReplaceableUnitMissing Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardMissing	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device detects that a provisioned card is not physically present.		
Remedial action: Informational - no corrective action required.		

Table 26-87 ReplaceableUnitMissing (mpr)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitMissing (635) Type: equipmentAlarm Package: mpr.ReplaceableUnitMissing Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardMissing	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a device detects that a provisioned MPT is not physically present.		
Remedial action: The alarm is raised when a device detects that a provisioned card is not physically present.		

Table 26-88 ReplaceableUnitProblem (equipment)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitProblem (636) Type: equipmentAlarm Package: equipment.ReplaceableUnitProblem Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a card fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-89 ReplaceableUnitProblem (mpr)

Alarm	Attributes	Applicable major release
Name: ReplaceableUnitProblem (636) Type: equipmentAlarm Package: mpr.ReplaceableUnitProblem Raised on class: mpr.SubRackElements	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a card fails.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-90 RxFail (equipment)

Alarm	Attributes	Applicable major release
Name: RxFail (687) Type: communicationsAlarm Package: equipment.RxFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-90 RxFail (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MSS detects a receive failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-91 RxFail (radioequipment)

Alarm	Attributes	Applicable major release
Name: RxFail (687) Type: communicationsAlarm Package: radioequipment.RxFail Raised on class: radioequipment.RadioPortSpecifics	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxFail	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an MSS detects a receive failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-92 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 26-93 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 26-94 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 26-95 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 26-96 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 26-97 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 26-98 SynchronizationSignalFailure

Alarm	Attributes	Applicable major release
Name: SynchronizationSignalFailure (2944) Type: communicationsAlarm Package: equipment.SynchronizationSignalFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: synchronizationSignalFailure	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a synchronization signal failure is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-99 TMNLossofSignal (netw)

Alarm	Attributes	Applicable major release
Name: TMNLossofSignal (1920) Type: communicationsAlarm Package: netw.TMNLossofSignal Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tmnLOS	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when a Loss of Signal occurs on the TMN Interface.		
Remedial action: Please refer to the 9500-1C/SA Node Maintenance manual for remedial action information.		

Table 26-100 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 26-101 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 26-102 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0

Table 26-102 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 26-103 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 26-104 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 26-105 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 26-106 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 26-107 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 26-108 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 26-109 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 26-110 VersionMismatch (equipment)

Alarm	Attributes	Applicable major release
Name: VersionMismatch (646) Type: equipmentAlarm Package: equipment.VersionMismatch Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 5.0.0 • 5.1.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when an ODU software version mismatch is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 26-111 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 5.0.0 • 5.2.0 • 6.0.0 • 6.1.0 • 7.0.0 • 7.1.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

27 9774 LMG

27.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 27-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 27-2 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 27-3 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 27-4 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 27-5 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 27-5 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 27-6 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 27-7 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 27-8 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 27-9 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 27-10 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 27-10 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 27-11 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 27-12 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 27-13 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-13 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 27-14 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 27-15 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 27-16 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 27-17 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 27-18 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 27-19 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 27-20 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 27-21 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 27-21 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 27-22 IK8000001

Alarm	Attributes	Applicable major release
Name: IK8000001 (6450) Type: processingErrorAlarm Package: lmg.IK8000001 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: I/O NAS access error Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This alarm is raised in case of right access problem, full disk or network error. Alarm to be cleared by the operator at the management system.\nReason: applicationSubsystemFailure		
Remedial action: Check the directory right or NAS status		

Table 27-23 IK8000002

Alarm	Attributes	Applicable major release
Name: IK8000002 (6451) Type: processingErrorAlarm Package: lmg.IK8000002 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: DataBase access error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This alarm is raised in case there is no connection with the database. Alarm is cleared by the system.\nReason: applicationSubsystemFailure		
Remedial action: Check the state of the database		

Table 27-24 IK8000003

Alarm	Attributes	Applicable major release
Name: IK8000003 (6452) Type: communicationsAlarm Package: lmg.IK8000003 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: HTTP communication failure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: This alarm is raised in case of connection failure to the remote module. Alarm is cleared by the system.\nReason: communicationsSubsystemFailure		
Remedial action: Check the status of the target server		

Table 27-25 IK8000005

Alarm	Attributes	Applicable major release
Name: IK8000005 (6453) Type: processingErrorAlarm Package: Img.IK8000005 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Provision Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: configurationOrCustomizationError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-26 IK8000006

Alarm	Attributes	Applicable major release
Name: IK8000006 (8250) Type: processingErrorAlarm Package: Img.IK8000006 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Max allowed resources reached Implicitly cleared: false Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG
Description: This alarm is raised in case there are no more resource available. Alarm to be cleared by the operator at the management system.\nReason: resourceAtOrNearingCapacity		
Remedial action: Check licence or provisioning file		

Table 27-27 IK8000008

Alarm	Attributes	Applicable major release
Name: IK8000008 (6454) Type: processingErrorAlarm Package: Img.IK8000008 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Session preparation error Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This alarm is raised in case of bearer activation error. Alarm to be cleared by the operator at the management system.\nReason: applicationSubsystemFailure		
Remedial action: Check method used, other alarms for further info		

Table 27-28 IK8000012

Alarm	Attributes	Applicable major release
Name: IK8000012 (6455) Type: processingErrorAlarm Package: Img.IK8000012 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Data Backup Failure Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG

Table 27-28 IK8000012 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when a scheduled lmgbackup fails.. Alarm is cleared by the system.\nReason: applicationSubsystem-Failure		
Remedial action: See the Backup log file to have details on the Data backup operation failure, correct the potential error before retrying the operation or contact Nokia Technical Support.		

Table 27-29 IK8000013

Alarm	Attributes	Applicable major release
Name: IK8000013 (8251) Type: processingErrorAlarm Package: lmg.IK8000013 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: communicationsSubsystemFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-30 IK8000014

Alarm	Attributes	Applicable major release
Name: IK8000014 (8252) Type: processingErrorAlarm Package: lmg.IK8000014 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: communicationsSubsystemFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-31 IK8000015

Alarm	Attributes	Applicable major release
Name: IK8000015 (8253) Type: processingErrorAlarm Package: lmg.IK8000015 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: communicationsSubsystemFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-32 IK8000100

Alarm	Attributes	Applicable major release
Name: IK8000100 (6456) Type: environmentalAlarm Package: lmg.IK8000100 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: MME not responding Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG
Description: This alarm is raised in case of no response from primary MME. Alarm is cleared by the system.\nReason: externalEquipmentFailure		
Remedial action: Check MME and network status		

Table 27-33 IK8000101

Alarm	Attributes	Applicable major release
Name: IK8000101 (8254) Type: environmentalAlarm Package: lmg.IK8000101 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: MME not responding Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of no response from all MME of a pool. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: MME not responding (all)		
Remedial action: Check MME and network status		

Table 27-34 IK8000102

Alarm	Attributes	Applicable major release
Name: IK8000102 (6457) Type: environmentalAlarm Package: lmg.IK8000102 Raised on class: lmg.CPlane	Severity: major Specific problem: Connection failure on SG-mb interface Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when diameter peer failure is detected by BMSC on SG-mb interface. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Connection failure on SG-mb interface (BMSC)		
Remedial action: Check Diameter configuration and network access		

Table 27-35 IK8000103

Alarm	Attributes	Applicable major release
Name: IK8000103 (6458) Type: environmentalAlarm Package: lmg.IK8000103 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Connection failure on SG-mb interface Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when diameter peer failure is detected by MBMS-GW on SG-mb interface. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Connection failure on SG-mb interface (MBMS-GW)		
Remedial action: Check Diameter configuration and network access		

Table 27-36 IK8000105

Alarm	Attributes	Applicable major release
Name: IK8000105 (9648) Type: communicationsAlarm Package: lmg.IK8000105 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: MME restart counter increment detected Implicitly cleared: true Default probable cause: unavailable	Release: • LR16.1.MG
Description: This event is raised when MME restart counter increment on the Sm interface has been detected\nReason: MME restart counter increment detected		
Remedial action: No action is required.		

Table 27-37 IK8000106

Alarm	Attributes	Applicable major release
Name: IK8000106 (6459) Type: environmentalAlarm Package: lmg.IK8000106 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Provision Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: externalEquipmentFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-38 IK8000107

Alarm	Attributes	Applicable major release
Name: IK8000107 (6460) Type: processingErrorAlarm Package: lmg.IK8000107 Raised on class: lmg.DownloadAgent	Severity: minor Specific problem: OnDemand file download failure Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is raised in case of failure to download OnDemand file. Alarm to be cleared by the operator at the management system.\nReason: OnDemand file download failure		
Remedial action: Check the URI file access		

Table 27-39 IK8000108

Alarm	Attributes	Applicable major release
Name: IK8000108 (6461) Type: processingErrorAlarm Package: lmg.IK8000108 Raised on class: lmg.UPlaneProxy	Severity: major Specific problem: Missing socket Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when there are no more socket available for SGi-mb interface. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Missing socket		
Remedial action: Check system resources on the MBMS-GW		

Table 27-40 IK8000109

Alarm	Attributes	Applicable major release
Name: IK8000109 (9057) Type: processingErrorAlarm Package: lmg.IK8000109 Raised on class: lmg.CPlane	Severity: major Specific problem: eMBMS session delete failure Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the BM-SC is unable to remove an eMBMS session. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: eMBMS session delete failure		
Remedial action: Check for other LMG alarms conditions that may have caused the session delete operation to fail. Session will need to be manually deleted.		

Table 27-41 IK8000110

Alarm	Attributes	Applicable major release
Name: IK8000110 (6462) Type: securityServiceOrMechanismViolation Package: Img.IK8000110 Raised on class: Img.DownloadAgent	Severity: major Specific problem: HTTP basic authentication error Implicitly cleared: true Default probable cause: authenticationFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of authentication error - DownloadAgent. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: HTTP basic authentication error		
Remedial action: Check right or authentication parameters		

Table 27-42 IK8000112

Alarm	Attributes	Applicable major release
Name: IK8000112 (9058) Type: processingErrorAlarm Package: Img.IK8000112 Raised on class: Img.CPlane	Severity: major Specific problem: Session Audit Failure Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the BM-SC has detected a session error. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Session Audit Failure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-43 IK8000113

Alarm	Attributes	Applicable major release
Name: IK8000113 (6463) Type: processingErrorAlarm Package: Img.IK8000113 Raised on class: Img.DownloadAgent	Severity: minor Specific problem: Problem with File Uri, or unreachable DNS Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the File Uri domain name cannot be resolved, or the file Uri cannot be found. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Problem with File Uri, or unreachable DNS		
Remedial action: Check DNS status, check content server or file availability		

Table 27-44 IK8000114

Alarm	Attributes	Applicable major release
Name: IK8000114 (9649) Type: communicationsAlarm Package: lmg.IK8000114 Raised on class: lmg.CPlaneProxy	Severity: indeterminate Specific problem: Session Start Failure in an MME pool Implicitly cleared: true Default probable cause: callSetUpFailure	Release: • LR16.1.MG
Description: This event is raised when MBMS-GW is unable to start a session in an MME pool\nReason: Session Start Failure in an MME pool		
Remedial action: No action is required.		

Table 27-45 IK8000115

Alarm	Attributes	Applicable major release
Name: IK8000115 (9059) Type: processingErrorAlarm Package: lmg.IK8000115 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Configuration file error on MBMS-GW Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: This alarm is raised when the LMG detects a configuration file error. Alarm is cleared by the system.\nReason: Configuration file error on MBMS-GW		
Remedial action: Check the LMG logs for error details		

Table 27-46 IK8000116

Alarm	Attributes	Applicable major release
Name: IK8000116 (9650) Type: processingErrorAlarm Package: lmg.IK8000116 Raised on class: lmg.CPlane	Severity: indeterminate Specific problem: Session Audit Failure Implicitly cleared: true Default probable cause: corruptData	Release: • LR16.1.MG
Description: This event is raised when the BM-SC has detected a session error\nReason: Session Audit Failure		
Remedial action: No action is required.		

Table 27-47 IK8000117

Alarm	Attributes	Applicable major release
Name: IK8000117 (6464) Type: environmentalAlarm Package: lmg.IK8000117 Raised on class: lmg.CPlane	Severity: minor Specific problem: No successful RAA Diameter message received Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when no successful RAA (start session/stop session) Diameter message is received from MBMS-GW. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: No successful RAA Diameter message received		
Remedial action: Check MBMS-GW and network status		

Table 27-48 IK8000118

Alarm	Attributes	Applicable major release
Name: IK8000118 (9060) Type: processingErrorAlarm Package: lmg.IK8000118 Raised on class: lmg.NetworkPlanning	Severity: major Specific problem: Configuration file error on BM-SC MDF Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: This alarm is raised when the LMG detects a configuration file error. Alarm is cleared by the system.\nReason: Configuration file error on BM-SC MDF		
Remedial action: Check the LMG logs for error details		

Table 27-49 IK8000119

Alarm	Attributes	Applicable major release
Name: IK8000119 (9061) Type: processingErrorAlarm Package: lmg.IK8000119 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Session Audit Failure Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.MG
Description: This alarm is raised when the MBMS-GW has detected a session error. Alarm is cleared by the system.\nReason: Session Audit Failure		
Remedial action: Contact Nokia technical support if the problem persists		

Table 27-50 IK8000120

Alarm	Attributes	Applicable major release
Name: IK8000120 (8255) Type: processingErrorAlarm Package: lmg.IK8000120 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: excessiveErrorRate		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-51 IK8000121

Alarm	Attributes	Applicable major release
Name: IK8000121 (8256) Type: processingErrorAlarm Package: lmg.IK8000121 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: excessiveErrorRate		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-52 IK8000122

Alarm	Attributes	Applicable major release
Name: IK8000122 (8257) Type: processingErrorAlarm Package: lmg.IK8000122 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: excessiveErrorRate		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-53 IK8000123

Alarm	Attributes	Applicable major release
Name: IK8000123 (8258) Type: processingErrorAlarm Package: lmg.IK8000123 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: excessiveErrorRate		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-54 IK8000124

Alarm	Attributes	Applicable major release
Name: IK8000124 (8259) Type: processingErrorAlarm Package: Img.IK8000124 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: excessiveErrorRate		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-55 IK8000130

Alarm	Attributes	Applicable major release
Name: IK8000130 (9062) Type: environmentalAlarm Package: Img.IK8000130 Raised on class: Img.SmLink	Severity: minor Specific problem: MME not responding Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR15.1.MG
Description: This alarm is raised in case of no response from primary MME. Alarm is cleared by the system.\nReason: MME not responding (primary)		
Remedial action: Check MME and network status		

Table 27-56 IK8000160

Alarm	Attributes	Applicable major release
Name: IK8000160 (10281) Type: processingErrorAlarm Package: Img.IK8000160 Raised on class: Img.LMGLM	Severity: warning Specific problem: License expiration approaching in next weeks Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the expiration date of a temporary license approaches (between 30 to 7 days). Alarm is cleared by the system when a new license is installed, or when a more sever alarm is raised, or when the service is restarted.\nReason: License expiration approaching in next weeks		
Remedial action: Install a new license		

Table 27-57 IK8000161

Alarm	Attributes	Applicable major release
Name: IK8000161 (10282) Type: processingErrorAlarm Package: lmg.IK8000161 Raised on class: lmg.LMGLM	Severity: major Specific problem: License expiration approaching in few days Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the expiration date of a temporary license approaches (between 7 to 1 days). Alarm is cleared by the system when a new license is installed, or when a more sever alarm is raised, or when the service is restarted.\nReason: License expiration approaching in few days		
Remedial action: Install a new license		

Table 27-58 IK8000162

Alarm	Attributes	Applicable major release
Name: IK8000162 (10283) Type: processingErrorAlarm Package: lmg.IK8000162 Raised on class: lmg.LMGLM	Severity: critical Specific problem: License expired Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when a temporary license expires. Alarm is cleared by the system when a new license is installed, or when the service is restarted.\nReason: License expired		
Remedial action: Install a new license		

Table 27-59 IK8000163

Alarm	Attributes	Applicable major release
Name: IK8000163 (10284) Type: processingErrorAlarm Package: lmg.IK8000163 Raised on class: lmg.LMGLM	Severity: indeterminate Specific problem: The installation of capacity is over the HW capacity limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This event is raised when there is an attempt to activate a capacity over the limit authorized by the HW\nReason: The installation of capacity is over the HW capacity limit		
Remedial action: No action is required.		

Table 27-60 IK8000164

Alarm	Attributes	Applicable major release
Name: IK8000164 (10285) Type: processingErrorAlarm Package: Img.IK8000164 Raised on class: Img.LMGLM	Severity: warning Specific problem: The number of type1 sessions is approaching the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type1 session is approaching the limit activated in the LMG. Alarm is cleared by the system when load is under the threshold, or when a more sever alarm is raised, or when the service is restarted.\nReason: The number of type1 sessions is approaching the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-61 IK8000165

Alarm	Attributes	Applicable major release
Name: IK8000165 (10286) Type: processingErrorAlarm Package: Img.IK8000165 Raised on class: Img.LMGLM	Severity: warning Specific problem: The number of type2 sessions is approaching the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type2 session is approaching the limit activated in the LMG. Alarm is cleared by the system when load is under the threshold, or when a more sever alarm is raised, or when the service is restarted.\nReason: The number of type2 sessions is approaching the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-62 IK8000166

Alarm	Attributes	Applicable major release
Name: IK8000166 (10287) Type: processingErrorAlarm Package: Img.IK8000166 Raised on class: Img.LMGLM	Severity: warning Specific problem: The number of type3 sessions is approaching the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type3 session is approaching the limit activated in the LMG. Alarm is cleared by the system when load is under the threshold, or when a more sever alarm is raised, or when the service is restarted.\nReason: The number of type3 sessions is approaching the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-63 IK8000167

Alarm	Attributes	Applicable major release
Name: IK8000167 (10288) Type: processingErrorAlarm Package: lmg.IK8000167 Raised on class: lmg.LMGLM	Severity: warning Specific problem: The number of simultaneous sessions is approaching the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of simultaneous delivery session instances is approaching the limit activated in the LMG. Alarm is cleared by the system when load is under the threshold, or when a more sever alarm is raised, or when the service is restarted.\nReason: The number of simultaneous sessions is approaching the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-64 IK8000169

Alarm	Attributes	Applicable major release
Name: IK8000169 (10289) Type: processingErrorAlarm Package: lmg.IK8000169 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of type1 sessions exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type1 session is exceeding the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of type1 sessions exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-65 IK8000170

Alarm	Attributes	Applicable major release
Name: IK8000170 (10290) Type: processingErrorAlarm Package: lmg.IK8000170 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of type2 sessions exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type2 session is exceeding the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of type2 sessions exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-66 IK8000171

Alarm	Attributes	Applicable major release
Name: IK8000171 (10291) Type: processingErrorAlarm Package: lmg.IK8000171 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of type3 sessions exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of delivery session instances for type3 session is exceeding the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of type3 sessions exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-67 IK8000172

Alarm	Attributes	Applicable major release
Name: IK8000172 (10292) Type: processingErrorAlarm Package: lmg.IK8000172 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of simultaneous sessions exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of simultaneous delivery session instances exceeds the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of simultaneous sessions exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-68 IK8000174

Alarm	Attributes	Applicable major release
Name: IK8000174 (10293) Type: processingErrorAlarm Package: lmg.IK8000174 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of repair requests received per second exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of repair requests received per second exceeds the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of repair requests received per second exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-69 IK8000175

Alarm	Attributes	Applicable major release
Name: IK8000175 (10294) Type: processingErrorAlarm Package: lmg.IK8000175 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of report requests received per second exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of report requests received per second exceeds the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of report requests received per second exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-70 IK8000176

Alarm	Attributes	Applicable major release
Name: IK8000176 (10295) Type: processingErrorAlarm Package: lmg.IK8000176 Raised on class: lmg.LMGLM	Severity: major Specific problem: The number of repair/report requests received per second exceeds the limit Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised when the number of repair/report requests received per second exceeds the limit activated in the LMG. Alarm is cleared by the system when load is decreasing or when capacity is increased, or when the service is restarted.\nReason: The number of repair/report requests received per second exceeds the limit		
Remedial action: Purchase and activate additional capacity		

Table 27-71 IK8000190

Alarm	Attributes	Applicable major release
Name: IK8000190 (9652) Type: processingErrorAlarm Package: lmg.IK8000190 Raised on class: lmg.SessionAudit	Severity: major Specific problem: Inactive eMBMS session detected on MBMS-GW Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when no traffic is detected for a session on the MBMS-GW. The interface (SGi-mb or M1) is indicated in the alarm. Alarm is cleared by the system when the eMBMS session is stopped or traffic is restored, or when the service is restarted.\nReason: Inactive eMBMS session detected on MBMS-GW		
Remedial action: Delete the eMBMS session or check the traffic source for the session		

Table 27-72 IK8000191

Alarm	Attributes	Applicable major release
Name: IK8000191 (9653) Type: processingErrorAlarm Package: Img.IK8000191 Raised on class: Img.SessionAudit	Severity: major Specific problem: Orphan eMBMS session detected Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when an orphan eMBMS session is detected. Alarm is cleared by the system when the orphan session is deleted, or when the service is restarted.\nReason: Orphan eMBMS session detected		
Remedial action: The orphan eMBMS session has to be deleted from UPlane		

Table 27-73 IK8000192

Alarm	Attributes	Applicable major release
Name: IK8000192 (9654) Type: processingErrorAlarm Package: Img.IK8000192 Raised on class: Img.SessionAudit	Severity: major Specific problem: Orphan FLUTE delivery session detected Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when an orphan FLUTE delivery session is detected. Alarm is cleared by the system when the orphan FLUTE delivery session is deleted, or when the service is restarted.\nReason: Orphan FLUTE delivery session detected		
Remedial action: The orphan FLUTE delivery session has to be deleted from FLUTE		

Table 27-74 IK8000193

Alarm	Attributes	Applicable major release
Name: IK8000193 (9655) Type: processingErrorAlarm Package: Img.IK8000193 Raised on class: Img.SessionAudit	Severity: major Specific problem: Orphan FLUTE delivery instance detected Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when an orphan FLUTE delivery instance is detected. Alarm is cleared by the system when the orphan delivery instance is deleted, or when the service is restarted.\nReason: Orphan FLUTE delivery instance detected		
Remedial action: The orphan FLUTE delivery instance has to be deleted from FLUTE		

Table 27-75 IK8000196

Alarm	Attributes	Applicable major release
Name: IK8000196 (9658) Type: processingErrorAlarm Package: lmg.IK8000196 Raised on class: lmg.SessionAudit	Severity: major Specific problem: Inactive eMBMS session detected on BM-SC SGi-mb interface Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when an eMBMS session has no traffic for an amount of time on SGi-mb interface of BMSC MDF side. Alarm is cleared by the system when the eMBMS session is stopped or traffic is restored, or when the service is restarted.\ nReason: Inactive eMBMS session detected on BM-SC SGi-mb interface		
Remedial action: Delete the eMBMS session or check the traffic source for the session		

Table 27-76 IK8000197

Alarm	Attributes	Applicable major release
Name: IK8000197 (9659) Type: processingErrorAlarm Package: lmg.IK8000197 Raised on class: lmg.SessionAudit	Severity: major Specific problem: Inactive delivery session instance on BMSC MDF WebDAV interface Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when no ingress traffic is detected for a delivery session instance on the BMSC node interface with the encoder. Alarm is cleared by the system when the delivery session instance is stopped, on remove content request, or when traffic is restored, or when the service is restarted.\nReason: Inactive delivery session instance on BMSC MDF WebDAV interface		
Remedial action: Stop the delivery session instance, remove content request or check the traffic source for the session		

Table 27-77 IK8000199

Alarm	Attributes	Applicable major release
Name: IK8000199 (9660) Type: communicationsAlarm Package: lmg.IK8000199 Raised on class: lmg.Orchestration	Severity: indeterminate Specific problem: NBI received with unrecognized PLMN ID Implicitly cleared: true Default probable cause: invalidMessageReceived	Release: • LR16.1.MG
Description: This event is sent when BMSC receives an NBI message containing unrecognized PLMN ID. The event identifies the unrecognized PLMN ID\nReason: NBI received with unrecognized PLMN ID		
Remedial action: No action is required.		

Table 27-78 IK8000200

Alarm	Attributes	Applicable major release
Name: IK8000200 (9661) Type: communicationsAlarm Package: lmg.IK8000200 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Sm Link session re-location trigger timer expired Implicitly cleared: true Default probable cause: communicationsReceiveFailure	Release: • LR16.1.MG
Description: This event is raised when due to an Sm Link failure, the LMG may be removing active sessions from this MME. Check MME and network status\nReason: Sm Link session re-location trigger timer expired		
Remedial action: No action is required.		

Table 27-79 IK8000201

Alarm	Attributes	Applicable major release
Name: IK8000201 (9662) Type: communicationsAlarm Package: lmg.IK8000201 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Sm Link non-transient failure timer expired Implicitly cleared: true Default probable cause: communicationsReceiveFailure	Release: • LR16.1.MG
Description: This event is raised when the Sm Link MME status is Inactive. Check MME and network status\nReason: Sm Link non-transient failure timer expired		
Remedial action: No action is required.		

Table 27-80 IK8000203

Alarm	Attributes	Applicable major release
Name: IK8000203 (10296) Type: communicationsAlarm Package: lmg.IK8000203 Raised on class: lmg.SmLink	Severity: minor Specific problem: MME not responding Implicitly cleared: true Default probable cause: communicationsReceiveFailure	Release: • LR16.1.MG
Description: This alarm is raised in case of no response from this MME. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: MME not responding (primary)		
Remedial action: Check MME and network status		

Table 27-81 IK8000500

Alarm	Attributes	Applicable major release
Name: IK8000500 (9063) Type: processingErrorAlarm Package: lmg.IK8000500 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-82 IK8000501

Alarm	Attributes	Applicable major release
Name: IK8000501 (9064) Type: processingErrorAlarm Package: lmg.IK8000501 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-83 IK8000502

Alarm	Attributes	Applicable major release
Name: IK8000502 (9065) Type: processingErrorAlarm Package: lmg.IK8000502 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-84 IK8000503

Alarm	Attributes	Applicable major release
Name: IK8000503 (9066) Type: processingErrorAlarm Package: lmg.IK8000503 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-85 IK8000504

Alarm	Attributes	Applicable major release
Name: IK8000504 (9067) Type: processingErrorAlarm Package: lmg.IK8000504 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-86 IK8000505

Alarm	Attributes	Applicable major release
Name: IK8000505 (9068) Type: processingErrorAlarm Package: lmg.IK8000505 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-87 IK8000506

Alarm	Attributes	Applicable major release
Name: IK8000506 (9069) Type: processingErrorAlarm Package: lmg.IK8000506 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-88 IK8000507

Alarm	Attributes	Applicable major release
Name: IK8000507 (9070) Type: processingErrorAlarm Package: lmg.IK8000507 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-89 IK8000508

Alarm	Attributes	Applicable major release
Name: IK8000508 (9071) Type: processingErrorAlarm Package: lmg.IK8000508 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-90 IK8000509

Alarm	Attributes	Applicable major release
Name: IK8000509 (9072) Type: processingErrorAlarm Package: lmg.IK8000509 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-91 IK8000510

Alarm	Attributes	Applicable major release
Name: IK8000510 (9073) Type: processingErrorAlarm Package: lmg.IK8000510 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-92 IK8000511

Alarm	Attributes	Applicable major release
Name: IK8000511 (9074) Type: processingErrorAlarm Package: lmg.IK8000511 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-93 IK8000512

Alarm	Attributes	Applicable major release
Name: IK8000512 (9075) Type: processingErrorAlarm Package: Img.IK8000512 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-94 IK8000513

Alarm	Attributes	Applicable major release
Name: IK8000513 (9076) Type: processingErrorAlarm Package: Img.IK8000513 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-95 IK8000514

Alarm	Attributes	Applicable major release
Name: IK8000514 (9077) Type: processingErrorAlarm Package: Img.IK8000514 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-96 IK8000515

Alarm	Attributes	Applicable major release
Name: IK8000515 (9078) Type: processingErrorAlarm Package: Img.IK8000515 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-97 IK8000516

Alarm	Attributes	Applicable major release
Name: IK8000516 (9079) Type: processingErrorAlarm Package: lmg.IK8000516 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-98 IK8000517

Alarm	Attributes	Applicable major release
Name: IK8000517 (9080) Type: processingErrorAlarm Package: lmg.IK8000517 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-99 IK8000518

Alarm	Attributes	Applicable major release
Name: IK8000518 (9081) Type: processingErrorAlarm Package: lmg.IK8000518 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-100 IK8000519

Alarm	Attributes	Applicable major release
Name: IK8000519 (9082) Type: processingErrorAlarm Package: lmg.IK8000519 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-101 IK8000520

Alarm	Attributes	Applicable major release
Name: IK8000520 (9083) Type: processingErrorAlarm Package: Img.IK8000520 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-102 IK8000521

Alarm	Attributes	Applicable major release
Name: IK8000521 (9084) Type: processingErrorAlarm Package: Img.IK8000521 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-103 IK8000522

Alarm	Attributes	Applicable major release
Name: IK8000522 (9085) Type: processingErrorAlarm Package: Img.IK8000522 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-104 IK8000523

Alarm	Attributes	Applicable major release
Name: IK8000523 (9086) Type: processingErrorAlarm Package: Img.IK8000523 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-105 IK8000524

Alarm	Attributes	Applicable major release
Name: IK8000524 (9087) Type: processingErrorAlarm Package: lmg.IK8000524 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-106 IK8000525

Alarm	Attributes	Applicable major release
Name: IK8000525 (9088) Type: processingErrorAlarm Package: lmg.IK8000525 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-107 IK8000526

Alarm	Attributes	Applicable major release
Name: IK8000526 (9089) Type: processingErrorAlarm Package: lmg.IK8000526 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-108 IK8000527

Alarm	Attributes	Applicable major release
Name: IK8000527 (9090) Type: processingErrorAlarm Package: lmg.IK8000527 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-109 IK8000528

Alarm	Attributes	Applicable major release
Name: IK8000528 (9091) Type: processingErrorAlarm Package: lmg.IK8000528 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-110 IK8000529

Alarm	Attributes	Applicable major release
Name: IK8000529 (9092) Type: processingErrorAlarm Package: lmg.IK8000529 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-111 IK8000530

Alarm	Attributes	Applicable major release
Name: IK8000530 (9093) Type: processingErrorAlarm Package: lmg.IK8000530 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-112 IK8000531

Alarm	Attributes	Applicable major release
Name: IK8000531 (9094) Type: processingErrorAlarm Package: lmg.IK8000531 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-113 IK8000532

Alarm	Attributes	Applicable major release
Name: IK8000532 (9095) Type: processingErrorAlarm Package: lmg.IK8000532 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-114 IK8000533

Alarm	Attributes	Applicable major release
Name: IK8000533 (9096) Type: processingErrorAlarm Package: lmg.IK8000533 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-115 IK8000534

Alarm	Attributes	Applicable major release
Name: IK8000534 (9097) Type: processingErrorAlarm Package: lmg.IK8000534 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-116 IK8000535

Alarm	Attributes	Applicable major release
Name: IK8000535 (9098) Type: processingErrorAlarm Package: lmg.IK8000535 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-117 IK8000536

Alarm	Attributes	Applicable major release
Name: IK8000536 (9099) Type: processingErrorAlarm Package: Img.IK8000536 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-118 IK8000537

Alarm	Attributes	Applicable major release
Name: IK8000537 (9100) Type: processingErrorAlarm Package: Img.IK8000537 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-119 IK8000538

Alarm	Attributes	Applicable major release
Name: IK8000538 (9101) Type: processingErrorAlarm Package: Img.IK8000538 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-120 IK8000539

Alarm	Attributes	Applicable major release
Name: IK8000539 (9102) Type: processingErrorAlarm Package: Img.IK8000539 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-121 IK8000540

Alarm	Attributes	Applicable major release
Name: IK8000540 (9103) Type: processingErrorAlarm Package: lmg.IK8000540 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-122 IK8000541

Alarm	Attributes	Applicable major release
Name: IK8000541 (9104) Type: processingErrorAlarm Package: lmg.IK8000541 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-123 IK8000542

Alarm	Attributes	Applicable major release
Name: IK8000542 (9105) Type: processingErrorAlarm Package: lmg.IK8000542 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-124 IK8000543

Alarm	Attributes	Applicable major release
Name: IK8000543 (9106) Type: processingErrorAlarm Package: lmg.IK8000543 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-125 IK8000544

Alarm	Attributes	Applicable major release
Name: IK8000544 (9107) Type: processingErrorAlarm Package: Img.IK8000544 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-126 IK8000545

Alarm	Attributes	Applicable major release
Name: IK8000545 (9108) Type: processingErrorAlarm Package: Img.IK8000545 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-127 IK8000546

Alarm	Attributes	Applicable major release
Name: IK8000546 (9109) Type: processingErrorAlarm Package: Img.IK8000546 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-128 IK8000547

Alarm	Attributes	Applicable major release
Name: IK8000547 (9110) Type: processingErrorAlarm Package: Img.IK8000547 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-129 IK8000548

Alarm	Attributes	Applicable major release
Name: IK8000548 (9111) Type: processingErrorAlarm Package: lmg.IK8000548 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-130 IK8000549

Alarm	Attributes	Applicable major release
Name: IK8000549 (9112) Type: processingErrorAlarm Package: lmg.IK8000549 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-131 IK8000550

Alarm	Attributes	Applicable major release
Name: IK8000550 (9663) Type: processingErrorAlarm Package: lmg.IK8000550 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-132 IK8000551

Alarm	Attributes	Applicable major release
Name: IK8000551 (9664) Type: processingErrorAlarm Package: lmg.IK8000551 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-133 IK8000552

Alarm	Attributes	Applicable major release
Name: IK8000552 (9665) Type: processingErrorAlarm Package: lmg.IK8000552 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-134 IK8000553

Alarm	Attributes	Applicable major release
Name: IK8000553 (9666) Type: processingErrorAlarm Package: lmg.IK8000553 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-135 IK8000554

Alarm	Attributes	Applicable major release
Name: IK8000554 (9667) Type: processingErrorAlarm Package: lmg.IK8000554 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-136 IK8000555

Alarm	Attributes	Applicable major release
Name: IK8000555 (9668) Type: processingErrorAlarm Package: lmg.IK8000555 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-137 IK8000556

Alarm	Attributes	Applicable major release
Name: IK8000556 (9669) Type: processingErrorAlarm Package: Img.IK8000556 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-138 IK8000557

Alarm	Attributes	Applicable major release
Name: IK8000557 (9670) Type: processingErrorAlarm Package: Img.IK8000557 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-139 IK8000558

Alarm	Attributes	Applicable major release
Name: IK8000558 (9671) Type: processingErrorAlarm Package: Img.IK8000558 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-140 IK8000559

Alarm	Attributes	Applicable major release
Name: IK8000559 (9672) Type: processingErrorAlarm Package: Img.IK8000559 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-141 IK8000560

Alarm	Attributes	Applicable major release
Name: IK8000560 (9673) Type: processingErrorAlarm Package: lmg.IK8000560 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-142 IK8000561

Alarm	Attributes	Applicable major release
Name: IK8000561 (9674) Type: processingErrorAlarm Package: lmg.IK8000561 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-143 IK8000562

Alarm	Attributes	Applicable major release
Name: IK8000562 (10297) Type: processingErrorAlarm Package: lmg.IK8000562 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-144 IK8000563

Alarm	Attributes	Applicable major release
Name: IK8000563 (10298) Type: processingErrorAlarm Package: lmg.IK8000563 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-145 IK8000564

Alarm	Attributes	Applicable major release
Name: IK8000564 (10299) Type: processingErrorAlarm Package: lmg.IK8000564 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-146 IK8000565

Alarm	Attributes	Applicable major release
Name: IK8000565 (10300) Type: processingErrorAlarm Package: lmg.IK8000565 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-147 IK8000566

Alarm	Attributes	Applicable major release
Name: IK8000566 (9675) Type: processingErrorAlarm Package: lmg.IK8000566 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-148 IK8000567

Alarm	Attributes	Applicable major release
Name: IK8000567 (9676) Type: processingErrorAlarm Package: lmg.IK8000567 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-149 IK8000568

Alarm	Attributes	Applicable major release
Name: IK8000568 (9677) Type: processingErrorAlarm Package: lmg.IK8000568 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-150 IK8000569

Alarm	Attributes	Applicable major release
Name: IK8000569 (9678) Type: processingErrorAlarm Package: lmg.IK8000569 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-151 IK8000570

Alarm	Attributes	Applicable major release
Name: IK8000570 (9679) Type: processingErrorAlarm Package: lmg.IK8000570 Raised on class: lmg.CPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-152 IK8000571

Alarm	Attributes	Applicable major release
Name: IK8000571 (9680) Type: processingErrorAlarm Package: lmg.IK8000571 Raised on class: lmg.CPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-153 IK8000572

Alarm	Attributes	Applicable major release
Name: IK8000572 (9681) Type: processingErrorAlarm Package: lmg.IK8000572 Raised on class: lmg.CPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-154 IK8000573

Alarm	Attributes	Applicable major release
Name: IK8000573 (9682) Type: processingErrorAlarm Package: lmg.IK8000573 Raised on class: lmg.CPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-155 IK8000574

Alarm	Attributes	Applicable major release
Name: IK8000574 (9683) Type: processingErrorAlarm Package: lmg.IK8000574 Raised on class: lmg.DownloadAgent	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-156 IK8000575

Alarm	Attributes	Applicable major release
Name: IK8000575 (9684) Type: processingErrorAlarm Package: lmg.IK8000575 Raised on class: lmg.DownloadAgent	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-157 IK8000576

Alarm	Attributes	Applicable major release
Name: IK8000576 (9685) Type: processingErrorAlarm Package: Img.IK8000576 Raised on class: Img.DownloadAgent	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-158 IK8000577

Alarm	Attributes	Applicable major release
Name: IK8000577 (9686) Type: processingErrorAlarm Package: Img.IK8000577 Raised on class: Img.DownloadAgent	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-159 IK8000578

Alarm	Attributes	Applicable major release
Name: IK8000578 (9687) Type: processingErrorAlarm Package: Img.IK8000578 Raised on class: Img.FRepairAndReport	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised when the disk space dedicated to daily reporting is full. Alarm is cleared when there is enough disk space for the daily reporting.\nReason: Disk space dedicated to daily reporting is full		
Remedial action: Free disk space		

Table 27-160 IK8000579

Alarm	Attributes	Applicable major release
Name: IK8000579 (9688) Type: processingErrorAlarm Package: Img.IK8000579 Raised on class: Img.FRepairAndReport	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-160 IK8000579 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when disk space dedicated to daily reporting has reached a threshold, percentage of the maximum value. Alarm is cleared when disk space dedicated to daily reporting is under 10% of the threshold.\nReason: Disk space dedicated to daily reporting has reached a threshold		
Remedial action: Free disk space		

Table 27-161 IK8000580

Alarm	Attributes	Applicable major release
Name: IK8000580 (9689) Type: processingErrorAlarm Package: lmg.IK8000580 Raised on class: lmg.FRepairAndReport	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-162 IK8000581

Alarm	Attributes	Applicable major release
Name: IK8000581 (9690) Type: processingErrorAlarm Package: lmg.IK8000581 Raised on class: lmg.FRepairAndReport	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-163 IK8000582

Alarm	Attributes	Applicable major release
Name: IK8000582 (9691) Type: processingErrorAlarm Package: lmg.IK8000582 Raised on class: lmg.LMGLM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-164 IK8000583

Alarm	Attributes	Applicable major release
Name: IK8000583 (9692) Type: processingErrorAlarm Package: lmg.IK8000583 Raised on class: lmg.LMGLM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-165 IK8000584

Alarm	Attributes	Applicable major release
Name: IK8000584 (9693) Type: processingErrorAlarm Package: lmg.IK8000584 Raised on class: lmg.LMGLM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-166 IK8000585

Alarm	Attributes	Applicable major release
Name: IK8000585 (9694) Type: processingErrorAlarm Package: lmg.IK8000585 Raised on class: lmg.LMGLM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-167 IK8000586

Alarm	Attributes	Applicable major release
Name: IK8000586 (9695) Type: processingErrorAlarm Package: lmg.IK8000586 Raised on class: lmg.NetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-168 IK8000587

Alarm	Attributes	Applicable major release
Name: IK8000587 (9696) Type: processingErrorAlarm Package: lmg.IK8000587 Raised on class: lmg.NetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-169 IK8000588

Alarm	Attributes	Applicable major release
Name: IK8000588 (9697) Type: processingErrorAlarm Package: lmg.IK8000588 Raised on class: lmg.NetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-170 IK8000589

Alarm	Attributes	Applicable major release
Name: IK8000589 (9698) Type: processingErrorAlarm Package: lmg.IK8000589 Raised on class: lmg.NetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-171 IK8000590

Alarm	Attributes	Applicable major release
Name: IK8000590 (9699) Type: processingErrorAlarm Package: lmg.IK8000590 Raised on class: lmg.OAM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-172 IK8000591

Alarm	Attributes	Applicable major release
Name: IK8000591 (9700) Type: processingErrorAlarm Package: Img.IK8000591 Raised on class: Img.OAM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-173 IK8000592

Alarm	Attributes	Applicable major release
Name: IK8000592 (9701) Type: processingErrorAlarm Package: Img.IK8000592 Raised on class: Img.OAM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-174 IK8000593

Alarm	Attributes	Applicable major release
Name: IK8000593 (9702) Type: processingErrorAlarm Package: Img.IK8000593 Raised on class: Img.OAM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-175 IK8000594

Alarm	Attributes	Applicable major release
Name: IK8000594 (9703) Type: processingErrorAlarm Package: Img.IK8000594 Raised on class: Img.Orchestration	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This event is raised when total throughput reached a threshold, percentage of the maximum authorized throughput\ nReason: Total throughput reached a threshold for specific broadcast window		
Remedial action: none		

Table 27-176 IK8000595

Alarm	Attributes	Applicable major release
Name: IK8000595 (9704) Type: processingErrorAlarm Package: lmg.IK8000595 Raised on class: lmg.Orchestration	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This event is raised when the number of active delivery sessions instances authorized by the license has reached a threshold, percentage of the maximum value\nReason: Total number of active delivery sessions instances reached a threshold for a broadcast window		
Remedial action: none		

Table 27-177 IK8000596

Alarm	Attributes	Applicable major release
Name: IK8000596 (9705) Type: processingErrorAlarm Package: lmg.IK8000596 Raised on class: lmg.Orchestration	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-178 IK8000597

Alarm	Attributes	Applicable major release
Name: IK8000597 (9706) Type: processingErrorAlarm Package: lmg.IK8000597 Raised on class: lmg.Orchestration	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-179 IK8000598

Alarm	Attributes	Applicable major release
Name: IK8000598 (9707) Type: processingErrorAlarm Package: lmg.IK8000598 Raised on class: lmg.SANEServiceProvider	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		

Table 27-179 IK8000598 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-180 IK8000599

Alarm	Attributes	Applicable major release
Name: IK8000599 (9708) Type: processingErrorAlarm Package: Img.IK8000599 Raised on class: Img.SANEServiceProvider	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-181 IK8000600

Alarm	Attributes	Applicable major release
Name: IK8000600 (9709) Type: processingErrorAlarm Package: Img.IK8000600 Raised on class: Img.SANEServiceProvider	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-182 IK8000601

Alarm	Attributes	Applicable major release
Name: IK8000601 (9710) Type: processingErrorAlarm Package: Img.IK8000601 Raised on class: Img.SANEServiceProvider	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-183 IK8000602

Alarm	Attributes	Applicable major release
Name: IK8000602 (9711) Type: processingErrorAlarm Package: lmg.IK8000602 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-184 IK8000603

Alarm	Attributes	Applicable major release
Name: IK8000603 (9712) Type: processingErrorAlarm Package: lmg.IK8000603 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-185 IK8000604

Alarm	Attributes	Applicable major release
Name: IK8000604 (9713) Type: processingErrorAlarm Package: lmg.IK8000604 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-186 IK8000605

Alarm	Attributes	Applicable major release
Name: IK8000605 (9714) Type: processingErrorAlarm Package: lmg.IK8000605 Raised on class: lmg.SmLink	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-187 IK8000606

Alarm	Attributes	Applicable major release
Name: IK8000606 (9715) Type: processingErrorAlarm Package: Img.IK8000606 Raised on class: Img.UPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-188 IK8000607

Alarm	Attributes	Applicable major release
Name: IK8000607 (9716) Type: processingErrorAlarm Package: Img.IK8000607 Raised on class: Img.UPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-189 IK8000608

Alarm	Attributes	Applicable major release
Name: IK8000608 (9717) Type: processingErrorAlarm Package: Img.IK8000608 Raised on class: Img.UPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-190 IK8000609

Alarm	Attributes	Applicable major release
Name: IK8000609 (9718) Type: processingErrorAlarm Package: Img.IK8000609 Raised on class: Img.UPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-191 IK8000610

Alarm	Attributes	Applicable major release
Name: IK8000610 (9719) Type: processingErrorAlarm Package: lmg.IK8000610 Raised on class: lmg.SessionAudit	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-192 IK8000611

Alarm	Attributes	Applicable major release
Name: IK8000611 (9720) Type: processingErrorAlarm Package: lmg.IK8000611 Raised on class: lmg.SessionAudit	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-193 IK8000612

Alarm	Attributes	Applicable major release
Name: IK8000612 (9721) Type: processingErrorAlarm Package: lmg.IK8000612 Raised on class: lmg.SessionAudit	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-194 IK8000613

Alarm	Attributes	Applicable major release
Name: IK8000613 (9722) Type: processingErrorAlarm Package: lmg.IK8000613 Raised on class: lmg.SessionAudit	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-195 IK8000614

Alarm	Attributes	Applicable major release
Name: IK8000614 (10301) Type: processingErrorAlarm Package: Img.IK8000614 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-196 IK8000615

Alarm	Attributes	Applicable major release
Name: IK8000615 (10302) Type: processingErrorAlarm Package: Img.IK8000615 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-197 IK8000616

Alarm	Attributes	Applicable major release
Name: IK8000616 (10303) Type: processingErrorAlarm Package: Img.IK8000616 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-198 IK8000617

Alarm	Attributes	Applicable major release
Name: IK8000617 (10304) Type: processingErrorAlarm Package: Img.IK8000617 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-199 IK8000618

Alarm	Attributes	Applicable major release
Name: IK8000618 (10305) Type: processingErrorAlarm Package: lmg.IK8000618 Raised on class: lmg.GwNetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-200 IK8000619

Alarm	Attributes	Applicable major release
Name: IK8000619 (10306) Type: processingErrorAlarm Package: lmg.IK8000619 Raised on class: lmg.GwNetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-201 IK8000620

Alarm	Attributes	Applicable major release
Name: IK8000620 (10307) Type: processingErrorAlarm Package: lmg.IK8000620 Raised on class: lmg.GwNetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-202 IK8000621

Alarm	Attributes	Applicable major release
Name: IK8000621 (10308) Type: processingErrorAlarm Package: lmg.IK8000621 Raised on class: lmg.GwNetworkPlanning	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-203 IK8000622

Alarm	Attributes	Applicable major release
Name: IK8000622 (10309) Type: processingErrorAlarm Package: Img.IK8000622 Raised on class: Img.CPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-204 IK8000623

Alarm	Attributes	Applicable major release
Name: IK8000623 (10310) Type: processingErrorAlarm Package: Img.IK8000623 Raised on class: Img.CPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-205 IK8000624

Alarm	Attributes	Applicable major release
Name: IK8000624 (10311) Type: processingErrorAlarm Package: Img.IK8000624 Raised on class: Img.CPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-206 IK8000625

Alarm	Attributes	Applicable major release
Name: IK8000625 (10312) Type: processingErrorAlarm Package: Img.IK8000625 Raised on class: Img.CPlaneProxy	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-207 IK8010106

Alarm	Attributes	Applicable major release
Name: IK8010106 (9113) Type: environmentalAlarm Package: Img.IK8010106 Raised on class: Img.Orchestration	Severity: major Specific problem: Service Provisioning Platform not responding Implicitly cleared: true Default probable cause: externalEquipmentFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of no response from BPS on NBI interface. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Service Provisioning Platform not responding		
Remedial action: Check Web services or Provisioning platform status		

Table 27-208 IK8010107

Alarm	Attributes	Applicable major release
Name: IK8010107 (10313) Type: processingErrorAlarm Package: Img.IK8010107 Raised on class: Img.DownloadAgent	Severity: minor Specific problem: OnDemand file download failure Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This alarm is raised in case of failure to download OnDemand file. Alarm is cleared by the system if the file can be downloaded or once the associated deliveryInstance is deleted, or when the service is restarted.\nReason: OnDemand file download failure		
Remedial action: Check the URI file access		

Table 27-209 IK8010120

Alarm	Attributes	Applicable major release
Name: IK8010120 (9114) Type: communicationsAlarm Package: Img.IK8010120 Raised on class: Img.DownloadAgent	Severity: warning Specific problem: Transaction error high for on demand content ingest Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when transaction error for on-demand content ingest is higher that requested threshold (success rate is defined as number of 200OK compared to number of addContent requests). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Transaction error high for on demand content ingest		
Remedial action: Diagnose Problem		

Table 27-210 IK8010121

Alarm	Attributes	Applicable major release
Name: IK8010121 (9115) Type: communicationsAlarm Package: lmg.IK8010121 Raised on class: lmg.DownloadAgent	Severity: warning Specific problem: Transaction error high for continuous content ingest Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when transaction error for continuous content ingest is higher that requested threshold (success rate is defined as number of 200OK compared to number of http PUT requests). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Transaction error high for continuous content ingest		
Remedial action: Diagnose Problem		

Table 27-211 IK8010122

Alarm	Attributes	Applicable major release
Name: IK8010122 (9116) Type: communicationsAlarm Package: lmg.IK8010122 Raised on class: lmg.CPlane	Severity: warning Specific problem: Transaction error high for SGmb transaction Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when transaction error for SGmb transaction is higher that requested threshold (success rate is defined as number of successful diameter RAA compared to number of RAR Start or Stop). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Transaction error high for SGmb transaction		
Remedial action: Diagnose Problem		

Table 27-212 IK8010123

Alarm	Attributes	Applicable major release
Name: IK8010123 (9117) Type: communicationsAlarm Package: lmg.IK8010123 Raised on class: lmg.FRepairAndReport	Severity: warning Specific problem: Repair error high Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when repair error is higher that requested threshold (success rate is defined as number of 200 OK compared to number of http GET from Ues). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Repair error high		
Remedial action: Diagnose Problem		

Table 27-213 IK8010124

Alarm	Attributes	Applicable major release
Name: IK8010124 (9118) Type: communicationsAlarm Package: lmg.IK8010124 Raised on class: lmg.FRepairAndReport	Severity: warning Specific problem: Reporting error high Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when reporting error is higher that requested threshold (success rate is defined as number of 200 OK compared to number of http PUT from Ues). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Reporting error high		
Remedial action: Diagnose Problem		

Table 27-214 IK8010510

Alarm	Attributes	Applicable major release
Name: IK8010510 (9119) Type: processingErrorAlarm Package: lmg.IK8010510 Raised on class: lmg.DownloadAgent	Severity: critical Specific problem: I/O NAS access error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of right access problem, full disk or network error. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: I/O NAS access error		
Remedial action: Check the directory right or NAS status		

Table 27-215 IK8010520

Alarm	Attributes	Applicable major release
Name: IK8010520 (9120) Type: processingErrorAlarm Package: lmg.IK8010520 Raised on class: lmg.Orchestration	Severity: major Specific problem: DataBase access error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case there is no connection with the database. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: DataBase access error		
Remedial action: Check the state of the database		

Table 27-216 IK8010521

Alarm	Attributes	Applicable major release
Name: IK8010521 (9121) Type: processingErrorAlarm Package: lmg.IK8010521 Raised on class: lmg.CPlane	Severity: major Specific problem: DataBase access error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG

Table 27-216 IK8010521 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised in case there is no connection with the database. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: DataBase access error		
Remedial action: Check the state of the database		

Table 27-217 IK8010522

Alarm	Attributes	Applicable major release
Name: IK8010522 (9122) Type: processingErrorAlarm Package: lmg.IK8010522 Raised on class: lmg.NetworkPlanning	Severity: major Specific problem: DataBase access error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case there is no connection with the database. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: DataBase access error		
Remedial action: Check the state of the database		

Table 27-218 IK8010531

Alarm	Attributes	Applicable major release
Name: IK8010531 (9123) Type: communicationsAlarm Package: lmg.IK8010531 Raised on class: lmg.CPlane	Severity: major Specific problem: HTTP communication failure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of connection failure to the remote module. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: HTTP communication failure		
Remedial action: Check the status of the target server		

Table 27-219 IK8010532

Alarm	Attributes	Applicable major release
Name: IK8010532 (9124) Type: communicationsAlarm Package: lmg.IK8010532 Raised on class: lmg.Orchestration	Severity: major Specific problem: HTTP communication failure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of connection failure to the remote module. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: HTTP communication failure		
Remedial action: Check the status of the target server		

Table 27-220 IK8010550

Alarm	Attributes	Applicable major release
Name: IK8010550 (9125) Type: processingErrorAlarm Package: lmg.IK8010550 Raised on class: lmg.NetworkPlanning	Severity: major Specific problem: Provisioning error Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of inconsistent or missing provisioning file. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Provisioning error		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-221 IK8010551

Alarm	Attributes	Applicable major release
Name: IK8010551 (9126) Type: processingErrorAlarm Package: lmg.IK8010551 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Provisioning error Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: This alarm is raised in case of inconsistent or missing provisioning file. Alarm is cleared by the system.\nReason: Provisioning error		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-222 IK8010552

Alarm	Attributes	Applicable major release
Name: IK8010552 (10314) Type: processingErrorAlarm Package: lmg.IK8010552 Raised on class: lmg.GwNetworkPlanning	Severity: major Specific problem: Provisioning error Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: This alarm is raised in case of inconsistent or missing provisioning file. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Provisioning error		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-223 IK8010560

Alarm	Attributes	Applicable major release
Name: IK8010560 (9127) Type: qualityOfServiceAlarm Package: Img.IK8010560 Raised on class: Img.NetworkPlanning	Severity: major Specific problem: Max allowed resources reached Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case there are no more resource available. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Max allowed resources reached		
Remedial action: Check licence or provisioning file		

Table 27-224 IK8010561

Alarm	Attributes	Applicable major release
Name: IK8010561 (9128) Type: qualityOfServiceAlarm Package: Img.IK8010561 Raised on class: Img.CPlaneProxy	Severity: major Specific problem: Max allowed resources reached Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • LR15.1.MG
Description: This alarm is raised in case there are no more resource available. Alarm is cleared by the system.\nReason: Max allowed resources reached		
Remedial action: Check licence or provisioning file		

Table 27-225 IK8010562

Alarm	Attributes	Applicable major release
Name: IK8010562 (10315) Type: qualityOfServiceAlarm Package: Img.IK8010562 Raised on class: Img.GwNetworkPlanning	Severity: major Specific problem: Max allowed resources reached Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • LR16.1.MG
Description: This alarm is raised in case there are no more resource available. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Max allowed resources reached		
Remedial action: Check licence or provisioning file		

Table 27-226 IK8010580

Alarm	Attributes	Applicable major release
Name: IK8010580 (9129) Type: processingErrorAlarm Package: Img.IK8010580 Raised on class: Img.CPlane	Severity: major Specific problem: Session preparation error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG

Table 27-226 IK8010580 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised in case of bearer activation error. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Session preparation error		
Remedial action: Check for other alarms and delete the bearer		

Table 27-227 IK8010581

Alarm	Attributes	Applicable major release
Name: IK8010581 (9130) Type: processingErrorAlarm Package: lmg.IK8010581 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Session preparation error Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This alarm is raised in case of bearer activation error. Alarm is cleared by the system.\nReason: Session preparation error		
Remedial action: Check for other alarms and delete the bearer		

Table 27-228 IK8010610

Alarm	Attributes	Applicable major release
Name: IK8010610 (9131) Type: securityServiceOrMechanismViolation Package: lmg.IK8010610 Raised on class: lmg.DownloadAgent	Severity: critical Specific problem: LMG X509 certificate has expired Implicitly cleared: false Default probable cause: nonRepudiationFailure	Release: • LR15.1.MG
Description: This alarm is raised when the X509 certificate has just expired. Certificate variables parameters are indicated in the alarm (e. G. Standard Version, Serial Number, Subject Info (Common name, CountryName, StateOrProvinceName, localityName, organizationName, organizationalUnitName, emailAddress), Issuer Info (Common name, CountryName, StateOrProvinceName, localityName, organizationName, organizationalUnitName, emailAddress), Expiration Date). Alarm to be cleared by the operator at the management system.\nReason: LMG X509 certificate has expired		
Remedial action: Update the LMG X509 certificate		

Table 27-229 IK8010611

Alarm	Attributes	Applicable major release
Name: IK8010611 (10316) Type: securityServiceOrMechanismViolation Package: lmg.IK8010611 Raised on class: lmg.DownloadAgent	Severity: critical Specific problem: LMG X509 certificate has expired Implicitly cleared: true Default probable cause: nonRepudiationFailure	Release: • LR16.1.MG
Description: This alarm is raised when the X509 certificate has just expired. Certificate variables parameters Standard Version, Serial Number, Subject Info, Issuer Info, and Expiration Date are indicated in the alarm.. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: LMG X509 certificate has expired		

Table 27-229 IK8010611 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Update the LMG X509 certificate		

Table 27-230 IK8010620

Alarm	Attributes	Applicable major release
Name: IK8010620 (9132) Type: processingErrorAlarm Package: lmg.IK8010620 Raised on class: lmg.OAM	Severity: major Specific problem: Data Backup Failure Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when a scheduled lmgbackup fails.. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Data Backup Failure		
Remedial action: See the Backup log file to have details on the Data backup operation failure, correct the potential error before retrying the operation or contact NOKIA customer support		

Table 27-231 IK8010630

Alarm	Attributes	Applicable major release
Name: IK8010630 (9133) Type: communicationsAlarm Package: lmg.IK8010630 Raised on class: lmg.SANEServiceProvider	Severity: critical Specific problem: Connection failure between GUI and server Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of connection failure between ServiceProvider and server (server can be CACTI, BPS, U-Plane, GSEM). Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Connection failure between GUI and server		
Remedial action: Verify if the ServiceProvider module is activated and well configured. Verify also if the server is on and well configured		

Table 27-232 IK8010640

Alarm	Attributes	Applicable major release
Name: IK8010640 (9134) Type: communicationsAlarm Package: lmg.IK8010640 Raised on class: lmg.SANEServiceProvider	Severity: critical Specific problem: Connection failure between LMG and SANE Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG

Table 27-232 IK8010640 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised in case of connection failure between LMG and SANE. Alarm to be cleared by the operator at the management system.\nReason: Connection failure between LMG and SANE		
Remedial action: Verify if the ServiceProvider module is activated and well configured. Verify also if the SANE servers and UDDI server is on and well configured		

Table 27-233 IK8010641

Alarm	Attributes	Applicable major release
Name: IK8010641 (10317) Type: communicationsAlarm Package: lmg.IK8010641 Raised on class: lmg.SANEServiceProvider	Severity: critical Specific problem: Connection failure between LMG and SANE Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm is raised in case of connection failure between LMG and SANE. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: Connection failure between LMG and SANE		
Remedial action: Verify if the ServiceProvider module is activated and well configured. Verify also if the SANE servers and UDDI server is on and well configured		

Table 27-234 IK8010650

Alarm	Attributes	Applicable major release
Name: IK8010650 (9135) Type: communicationsAlarm Package: lmg.IK8010650 Raised on class: lmg.SANEServiceProvider	Severity: critical Specific problem: non synchronization between SANE and service provider databases Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm is raised in case of non synchronization between service provider and SANE roles and users. Alarm to be cleared by the operator at the management system.\nReason: non synchronization between SANE and service provider databases		
Remedial action: Verify if the database of service provider module is well configured		

Table 27-235 IK8010651

Alarm	Attributes	Applicable major release
Name: IK8010651 (10318) Type: communicationsAlarm Package: lmg.IK8010651 Raised on class: lmg.SANEServiceProvider	Severity: critical Specific problem: non synchronization between SANE and service provider databases Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm is raised in case of non synchronization between service provider and SANE roles and users. Alarm is cleared by the system when alarmCode and MOI criterias are fulfilled, or when the service is restarted.\nReason: non synchronization between SANE and service provider databases		
Remedial action: Verify if the database of service provider module is well configured		

Table 27-236 IK8010750

Alarm	Attributes	Applicable major release
Name: IK8010750 (9136) Type: processingErrorAlarm Package: lmg.IK8010750 Raised on class: lmg.CPlaneProxy	Severity: major Specific problem: Missing IP address in M1 interface configuration Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of missing IPv4 or IPv6 address in the M1 interface configuration with dual stack enabled. Alarm is cleared by the system when the service is restarted.\nReason: Missing IP address in M1 interface configuration		
Remedial action: Configure MBMS-GW with missing IP address		

Table 27-237 IK8020002

Alarm	Attributes	Applicable major release
Name: IK8020002 (8260) Type: securityServiceOrMechanismViolation Package: lmg.IK8020002 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: Operator login failure Implicitly cleared: true Default probable cause: unauthorizedAccessAttempt	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of login failure after number of authorized failures. Alarm is cleared only after BPS restart.\nReason: Operator login failure		
Remedial action: Check BPS logs.		

Table 27-238 IK8020003

Alarm	Attributes	Applicable major release
Name: IK8020003 (8261) Type: communicationsAlarm Package: lmg.IK8020003 Raised on class: lmg.BpsFunction	Severity: major Specific problem: Unexpected major event at service execution Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when an unexpected BM-SC event occurs at least for an eMBMS session involving the complete (delivery) stop of the eMBMS service. Alarm is cleared only after BPS restart.\nReason: Unexpected major event at service execution		
Remedial action: check also alarms at BM-SC		

Table 27-239 IK8020004

Alarm	Attributes	Applicable major release
Name: IK8020004 (8262) Type: communicationsAlarm Package: lmg.IK8020004 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: Unexpected minor event at service execution Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when an unexpected BM-SC event occurs during an eMBMS session (e. G time-out on notification event) without disrupting the delivery of the eMBMS service. Alarm is cleared only after BPS restart.\nReason: Unexpected minor event at service execution		
Remedial action: check also alarms at BM-SC		

Table 27-240 IK8020005

Alarm	Attributes	Applicable major release
Name: IK8020005 (8263) Type: processingErrorAlarm Package: lmg.IK8020005 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: File scheduling overlap Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the start date of the next file to deliver is overlapping the delivery end date of the previous file. Alarm is cleared only after BPS restart.\nReason: File scheduling overlap		
Remedial action: The operator shall take care of the file size (and the delivery bitrate) when scheduling file delivery		

Table 27-241 IK8020006

Alarm	Attributes	Applicable major release
Name: IK8020006 (8264) Type: processingErrorAlarm Package: Img.IK8020006 Raised on class: Img.BpsFunction	Severity: major Specific problem: Service template not found Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the associated service template can not be found or opened. Alarm is cleared only after BPS restart.\nReason: Service template not found		
Remedial action: Restore the service template file		

Table 27-242 IK8020007

Alarm	Attributes	Applicable major release
Name: IK8020007 (8265) Type: processingErrorAlarm Package: Img.IK8020007 Raised on class: Img.BpsFunction	Severity: major Specific problem: Service template parsing error Implicitly cleared: true Default probable cause: corruptData	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the associated service template can not be interpreted successfullly. Alarm is cleared only after BPS restart.\nReason: Service template parsing error		
Remedial action: Restore the service template file		

Table 27-243 IK8020008

Alarm	Attributes	Applicable major release
Name: IK8020008 (8266) Type: processingErrorAlarm Package: Img.IK8020008 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-244 IK8020009

Alarm	Attributes	Applicable major release
Name: IK8020009 (8267) Type: communicationsAlarm Package: lmg.IK8020009 Raised on class: lmg.BpsFunction	Severity: major Specific problem: BM-SC unavailable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case all TCP connections (1 connection per active eMBMS session) with BM-SC fail. Alarm is cleared by the system.\nReason: BM-SC unavailable		
Remedial action: Check configured BM-SC within BPS		

Table 27-245 IK8020010

Alarm	Attributes	Applicable major release
Name: IK8020010 (8268) Type: communicationsAlarm Package: lmg.IK8020010 Raised on class: lmg.BpsFunction	Severity: major Specific problem: HTTP transaction error on NBI Implicitly cleared: true Default probable cause: callSetUpFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when BPS receives something other than 200-OK/201-Created in HTTP response from BMSC, for anything BPS initiates over the NBI.. Alarm is cleared only after BPS restart.\nReason: HTTP transaction error on NBI		
Remedial action: Check also alarms at BM-SC		

Table 27-246 IK8020011

Alarm	Attributes	Applicable major release
Name: IK8020011 (8269) Type: communicationsAlarm Package: lmg.IK8020011 Raised on class: lmg.BpsFunction	Severity: major Specific problem: BEARER CHECK TIME failure Implicitly cleared: true Default probable cause: timeoutExpired	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when BEARER CHECK TIME check failed. Alarm is cleared only after BPS restart.\nReason: BEARER CHECK TIME failure		
Remedial action: Check also alarms at BM-SC		

Table 27-247 IK8020012

Alarm	Attributes	Applicable major release
Name: IK8020012 (8270) Type: communicationsAlarm Package: lmg.IK8020012 Raised on class: lmg.BpsFunction	Severity: major Specific problem: BEARER CHECK TIME missing Implicitly cleared: true Default probable cause: timeoutExpired	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when BEARER CHECK TIME indication failed to arrive from BM-SC. Alarm is cleared only after BPS restart.\nReason: BEARER CHECK TIME missing		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-248 IK8020013

Alarm	Attributes	Applicable major release
Name: IK8020013 (8271) Type: processingErrorAlarm Package: lmg.IK8020013 Raised on class: lmg.BpsFunction	Severity: major Specific problem: Session database synchronization error Implicitly cleared: true Default probable cause: corruptData	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when an error is encountered while session database synchronization. Alarm is cleared only after BPS restart.\nReason: Session database synchronization error		
Remedial action: Manual corrective action via the BPS service provisioning. If the problem persists, contact NOKIA customer support.		

Table 27-249 IK8020014

Alarm	Attributes	Applicable major release
Name: IK8020014 (8272) Type: processingErrorAlarm Package: lmg.IK8020014 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: On demand file size unknown Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when file size cannot be determined to see if file can be delivered within specified time window. Alarm is cleared only after BPS restart.\nReason: On demand file size unknown		
Remedial action: Operator dependent. contact NOKIA customer support.		

Table 27-250 IK8020015

Alarm	Attributes	Applicable major release
Name: IK8020015 (8273) Type: processingErrorAlarm Package: lmg.IK8020015 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: This is a spare for future use\nReason: applicationSubsystemFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-251 IK8020016

Alarm	Attributes	Applicable major release
Name: IK8020016 (8274) Type: processingErrorAlarm Package: lmg.IK8020016 Raised on class: lmg.BpsFunction	Severity: major Specific problem: Session removed due to service area removal Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when session is removed because new service area database retrieved from SAM no longer contains one or more service areas that the session was scheduled to broadcast in. Alarm is cleared only after BPS restart.\nReason: Session removed due to service area removal		
Remedial action: Confirm SAI configuration		

Table 27-252 IK8020017

Alarm	Attributes	Applicable major release
Name: IK8020017 (8275) Type: processingErrorAlarm Package: lmg.IK8020017 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: Session may be impacted due to service area property change Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when session is impacted by discrepancy in new service area database retrieved from SAM. Alarm is cleared only after BPS restart.\nReason: Session may be impacted due to service area property change		
Remedial action: Confirm SAI configuration		

Table 27-253 IK8020018

Alarm	Attributes	Applicable major release
Name: IK8020018 (8276) Type: processingErrorAlarm Package: Img.IK8020018 Raised on class: Img.BpsFunction	Severity: critical Specific problem: BPS license not found Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The license file is not found. Alarm is cleared only after BPS restart.\nReason: BPS license not found		
Remedial action: Check . Lic file existence in and configDirPath		

Table 27-254 IK8020019

Alarm	Attributes	Applicable major release
Name: IK8020019 (8277) Type: processingErrorAlarm Package: Img.IK8020019 Raised on class: Img.BpsFunction	Severity: critical Specific problem: Problem with the BPS license Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The license file can not be parsed. Alarm is cleared only after BPS restart.\nReason: Problem with the BPS license		
Remedial action: Check that . Lic file is correct		

Table 27-255 IK8020020

Alarm	Attributes	Applicable major release
Name: IK8020020 (8278) Type: processingErrorAlarm Package: Img.IK8020020 Raised on class: Img.BpsFunction	Severity: critical Specific problem: USB key protection error Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: usb dongle check failed. Alarm is cleared only after BPS restart.\nReason: USB key protection error		
Remedial action: Check logs for more details.		

Table 27-256 IK8020021

Alarm	Attributes	Applicable major release
Name: IK8020021 (8279) Type: processingErrorAlarm Package: Img.IK8020021 Raised on class: Img.BpsFunction	Severity: critical Specific problem: BPS license invalid Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-256 IK8020021 (continued)

Alarm	Attributes	Applicable major release
Description: The license file is not valid for this server and/or software. Alarm is cleared only after BPS restart.\nReason: BPS license invalid		
Remedial action: Check that . Lic file is correct		

Table 27-257 IK8020022

Alarm	Attributes	Applicable major release
Name: IK8020022 (8280) Type: processingErrorAlarm Package: lmg.IK8020022 Raised on class: lmg.BpsFunction	Severity: critical Specific problem: BPS license expiration Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The license file is expired. Alarm is cleared only after BPS restart.\nReason: BPS license expiration		
Remedial action: Renew the license		

Table 27-258 IK8020023

Alarm	Attributes	Applicable major release
Name: IK8020023 (8281) Type: processingErrorAlarm Package: lmg.IK8020023 Raised on class: lmg.BpsFunction	Severity: critical Specific problem: Problem with the database. Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Can not open a database connection. Alarm is cleared only after BPS restart.\nReason: Problem with the database.		
Remedial action: Check that the database is started		

Table 27-259 IK8020024

Alarm	Attributes	Applicable major release
Name: IK8020024 (8282) Type: processingErrorAlarm Package: lmg.IK8020024 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: USB key protection warning Implicitly cleared: true Default probable cause: underlayingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Entering grace period. Alarm is cleared by the system.\nReason: USB key protection warning		
Remedial action: Check that the dongle is plugged		

Table 27-260 IK8020025

Alarm	Attributes	Applicable major release
Name: IK8020025 (8283) Type: processingErrorAlarm Package: Img.IK8020025 Raised on class: Img.BpsFunction	Severity: critical Specific problem: Problem with a database request Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A request can not be performed. Alarm is cleared only after BPS restart.\nReason: Problem with a database request		
Remedial action: Check that the database has been correctly installed.		

Table 27-261 IK8020026

Alarm	Attributes	Applicable major release
Name: IK8020026 (8284) Type: processingErrorAlarm Package: Img.IK8020026 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-262 IK8020027

Alarm	Attributes	Applicable major release
Name: IK8020027 (8285) Type: communicationsAlarm Package: Img.IK8020027 Raised on class: Img.BpsFunction	Severity: major Specific problem: SAM ingestion timeout Implicitly cleared: true Default probable cause: timeoutExpired	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Getting data from SAM exceeds defined time limitation. Alarm is cleared by the system.\nReason: SAM ingestion timeout		
Remedial action: Check the server. Log file		

Table 27-263 IK8020028

Alarm	Attributes	Applicable major release
Name: IK8020028 (8286) Type: communicationsAlarm Package: Img.IK8020028 Raised on class: Img.BpsFunction	Severity: major Specific problem: SAM-O connection error Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-263 IK8020028 (continued)

Alarm	Attributes	Applicable major release
Description: Cannot retrieve data from SAM server. Alarm is cleared by the system.\nReason: SAM-O connection error		
Remedial action: Check the server. Log file		

Table 27-264 IK8020029

Alarm	Attributes	Applicable major release
Name: IK8020029 (8287) Type: communicationsAlarm Package: Img.IK8020029 Raised on class: Img.BpsFunction	Severity: major Specific problem: Interface of BPS for SAM ingestion error Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Cannot post data to BPS server. Alarm is cleared by the system.\nReason: Interface of BPS for SAM ingestion error		
Remedial action: Check the server. Log file		

Table 27-265 IK8020030

Alarm	Attributes	Applicable major release
Name: IK8020030 (9137) Type: processingErrorAlarm Package: Img.IK8020030 Raised on class: Img.BpsFunction	Severity: minor Specific problem: eMBMS session not admitted Implicitly cleared: true Default probable cause: systemResourcesOverload	Release: • LR15.1.MG
Description: This alarm is raised when a MCE failed to admit an eMBMS session. Alarm is cleared by the system.\nReason: eMBMS session not admitted		
Remedial action: Operator should investigate potential impact to session quality		

Table 27-266 IK8020031

Alarm	Attributes	Applicable major release
Name: IK8020031 (9138) Type: communicationsAlarm Package: Img.IK8020031 Raised on class: Img.BpsFunction	Severity: minor Specific problem: eMBMS session cell down Implicitly cleared: true Default probable cause: unavailable	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when a cell handling eMBMS session is down. Alarm is cleared by the system.\nReason: eMBMS session cell down		
Remedial action: Operator should investigate potential impact to session quality		

Table 27-267 IK8020032

Alarm	Attributes	Applicable major release
Name: IK8020032 (9139) Type: communicationsAlarm Package: lmg.IK8020032 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: eMBMS session excessive M1 error Implicitly cleared: true Default probable cause: excessiveErrorRate	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when a eMBMS session is experiencing excessive M1 error. Alarm is cleared by the system.\ nReason: eMBMS session excessive M1 error		
Remedial action: Operator should investigate potential impact to session quality		

Table 27-268 IK8020033

Alarm	Attributes	Applicable major release
Name: IK8020033 (9140) Type: communicationsAlarm Package: lmg.IK8020033 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: M3 error Implicitly cleared: true Default probable cause: unavailable	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when a MCE sees M3 error. Alarm is cleared by the system.\nReason: M3 error		
Remedial action: Operator should investigate potential impact to session quality		

Table 27-269 IK8020034

Alarm	Attributes	Applicable major release
Name: IK8020034 (9141) Type: communicationsAlarm Package: lmg.IK8020034 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: SAM interface down Implicitly cleared: true Default probable cause: unavailable	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when JMS or SAM-O interface is down towards a SAM. Alarm is cleared by the system.\nReason: SAM interface down		
Remedial action: Operator should investigate the SAM or the network to SAM		

Table 27-270 IK8020035

Alarm	Attributes	Applicable major release
Name: IK8020035 (9142) Type: qualityOfServiceAlarm Package: lmg.IK8020035 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: Unicast consumption high Implicitly cleared: true Default probable cause: congestion	Release: • LR15.1.MG • LR16.1.MG

Table 27-270 IK8020035 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when current unicast consumption in the cell is too high to safely support eMBMS sessions. Alarm is cleared by the system.\nReason: Unicast consumption high		
Remedial action: Operator should investigate if there is a need to manually cancel a session		

Table 27-271 IK8020036

Alarm	Attributes	Applicable major release
Name: IK8020036 (9143) Type: processingErrorAlarm Package: Img.IK8020036 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-272 IK8020037

Alarm	Attributes	Applicable major release
Name: IK8020037 (9144) Type: processingErrorAlarm Package: Img.IK8020037 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-273 IK8020038

Alarm	Attributes	Applicable major release
Name: IK8020038 (9145) Type: processingErrorAlarm Package: Img.IK8020038 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-274 IK8020039

Alarm	Attributes	Applicable major release
Name: IK8020039 (9146) Type: processingErrorAlarm Package: lmg.IK8020039 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-275 IK8020040

Alarm	Attributes	Applicable major release
Name: IK8020040 (9147) Type: processingErrorAlarm Package: lmg.IK8020040 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-276 IK8020041

Alarm	Attributes	Applicable major release
Name: IK8020041 (9148) Type: processingErrorAlarm Package: lmg.IK8020041 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-277 IK8020042

Alarm	Attributes	Applicable major release
Name: IK8020042 (9149) Type: processingErrorAlarm Package: lmg.IK8020042 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-278 IK8020043

Alarm	Attributes	Applicable major release
Name: IK8020043 (9150) Type: processingErrorAlarm Package: lmg.IK8020043 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-279 IK8020044

Alarm	Attributes	Applicable major release
Name: IK8020044 (9151) Type: processingErrorAlarm Package: lmg.IK8020044 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-280 IK8020045

Alarm	Attributes	Applicable major release
Name: IK8020045 (9152) Type: processingErrorAlarm Package: lmg.IK8020045 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-281 IK8020046

Alarm	Attributes	Applicable major release
Name: IK8020046 (9153) Type: processingErrorAlarm Package: lmg.IK8020046 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-282 IK8020047

Alarm	Attributes	Applicable major release
Name: IK8020047 (9154) Type: processingErrorAlarm Package: lmg.IK8020047 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-283 IK8020048

Alarm	Attributes	Applicable major release
Name: IK8020048 (9155) Type: processingErrorAlarm Package: lmg.IK8020048 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-284 IK8020049

Alarm	Attributes	Applicable major release
Name: IK8020049 (9156) Type: processingErrorAlarm Package: lmg.IK8020049 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-285 IK8020050

Alarm	Attributes	Applicable major release
Name: IK8020050 (9157) Type: processingErrorAlarm Package: lmg.IK8020050 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-286 IK8020051

Alarm	Attributes	Applicable major release
Name: IK8020051 (9158) Type: processingErrorAlarm Package: lmg.IK8020051 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-287 IK8020052

Alarm	Attributes	Applicable major release
Name: IK8020052 (9159) Type: processingErrorAlarm Package: lmg.IK8020052 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-288 IK8020053

Alarm	Attributes	Applicable major release
Name: IK8020053 (9160) Type: processingErrorAlarm Package: lmg.IK8020053 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-289 IK8020054

Alarm	Attributes	Applicable major release
Name: IK8020054 (9161) Type: processingErrorAlarm Package: lmg.IK8020054 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-290 IK8020055

Alarm	Attributes	Applicable major release
Name: IK8020055 (9162) Type: processingErrorAlarm Package: Img.IK8020055 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-291 IK8020056

Alarm	Attributes	Applicable major release
Name: IK8020056 (9163) Type: processingErrorAlarm Package: Img.IK8020056 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-292 IK8020057

Alarm	Attributes	Applicable major release
Name: IK8020057 (9164) Type: processingErrorAlarm Package: Img.IK8020057 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-293 IK8020058

Alarm	Attributes	Applicable major release
Name: IK8020058 (9165) Type: processingErrorAlarm Package: Img.IK8020058 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-294 IK8020059

Alarm	Attributes	Applicable major release
Name: IK8020059 (9166) Type: processingErrorAlarm Package: lmg.IK8020059 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-295 IK8020060

Alarm	Attributes	Applicable major release
Name: IK8020060 (9167) Type: processingErrorAlarm Package: lmg.IK8020060 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-296 IK8020061

Alarm	Attributes	Applicable major release
Name: IK8020061 (9168) Type: processingErrorAlarm Package: lmg.IK8020061 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-297 IK8020062

Alarm	Attributes	Applicable major release
Name: IK8020062 (9169) Type: processingErrorAlarm Package: lmg.IK8020062 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-298 IK8020063

Alarm	Attributes	Applicable major release
Name: IK8020063 (9170) Type: processingErrorAlarm Package: Img.IK8020063 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-299 IK8020064

Alarm	Attributes	Applicable major release
Name: IK8020064 (9171) Type: processingErrorAlarm Package: Img.IK8020064 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-300 IK8020065

Alarm	Attributes	Applicable major release
Name: IK8020065 (9172) Type: processingErrorAlarm Package: Img.IK8020065 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-301 IK8020066

Alarm	Attributes	Applicable major release
Name: IK8020066 (9173) Type: processingErrorAlarm Package: Img.IK8020066 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-302 IK8020067

Alarm	Attributes	Applicable major release
Name: IK8020067 (9174) Type: processingErrorAlarm Package: lmg.IK8020067 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-303 IK8020068

Alarm	Attributes	Applicable major release
Name: IK8020068 (9175) Type: processingErrorAlarm Package: lmg.IK8020068 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-304 IK8020069

Alarm	Attributes	Applicable major release
Name: IK8020069 (9176) Type: processingErrorAlarm Package: lmg.IK8020069 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-305 IK8020070

Alarm	Attributes	Applicable major release
Name: IK8020070 (9177) Type: processingErrorAlarm Package: lmg.IK8020070 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-306 IK8020071

Alarm	Attributes	Applicable major release
Name: IK8020071 (9178) Type: processingErrorAlarm Package: lmg.IK8020071 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-307 IK8020072

Alarm	Attributes	Applicable major release
Name: IK8020072 (9179) Type: processingErrorAlarm Package: lmg.IK8020072 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-308 IK8020073

Alarm	Attributes	Applicable major release
Name: IK8020073 (9180) Type: processingErrorAlarm Package: lmg.IK8020073 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-309 IK8020074

Alarm	Attributes	Applicable major release
Name: IK8020074 (9181) Type: processingErrorAlarm Package: lmg.IK8020074 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-310 IK8020075

Alarm	Attributes	Applicable major release
Name: IK8020075 (9182) Type: processingErrorAlarm Package: lmg.IK8020075 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-311 IK8020076

Alarm	Attributes	Applicable major release
Name: IK8020076 (9183) Type: processingErrorAlarm Package: lmg.IK8020076 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-312 IK8020077

Alarm	Attributes	Applicable major release
Name: IK8020077 (9184) Type: processingErrorAlarm Package: lmg.IK8020077 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-313 IK8020078

Alarm	Attributes	Applicable major release
Name: IK8020078 (9185) Type: processingErrorAlarm Package: lmg.IK8020078 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-314 IK8020079

Alarm	Attributes	Applicable major release
Name: IK8020079 (9186) Type: processingErrorAlarm Package: Img.IK8020079 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-315 IK8020080

Alarm	Attributes	Applicable major release
Name: IK8020080 (9187) Type: processingErrorAlarm Package: Img.IK8020080 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-316 IK8020081

Alarm	Attributes	Applicable major release
Name: IK8020081 (9188) Type: processingErrorAlarm Package: Img.IK8020081 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-317 IK8020082

Alarm	Attributes	Applicable major release
Name: IK8020082 (9189) Type: processingErrorAlarm Package: Img.IK8020082 Raised on class: Img.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-318 IK8020083

Alarm	Attributes	Applicable major release
Name: IK8020083 (9190) Type: processingErrorAlarm Package: lmg.IK8020083 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-319 IK8020084

Alarm	Attributes	Applicable major release
Name: IK8020084 (9191) Type: processingErrorAlarm Package: lmg.IK8020084 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-320 IK8020085

Alarm	Attributes	Applicable major release
Name: IK8020085 (9192) Type: processingErrorAlarm Package: lmg.IK8020085 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-321 IK8020086

Alarm	Attributes	Applicable major release
Name: IK8020086 (9193) Type: processingErrorAlarm Package: lmg.IK8020086 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-322 IK8020087

Alarm	Attributes	Applicable major release
Name: IK8020087 (9194) Type: processingErrorAlarm Package: lmg.IK8020087 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-323 IK8020088

Alarm	Attributes	Applicable major release
Name: IK8020088 (9195) Type: processingErrorAlarm Package: lmg.IK8020088 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-324 IK8020089

Alarm	Attributes	Applicable major release
Name: IK8020089 (9196) Type: processingErrorAlarm Package: lmg.IK8020089 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-325 IK8020090

Alarm	Attributes	Applicable major release
Name: IK8020090 (9197) Type: processingErrorAlarm Package: lmg.IK8020090 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-326 IK8020091

Alarm	Attributes	Applicable major release
Name: IK8020091 (9198) Type: processingErrorAlarm Package: lmg.IK8020091 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-327 IK8020092

Alarm	Attributes	Applicable major release
Name: IK8020092 (9199) Type: processingErrorAlarm Package: lmg.IK8020092 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-328 IK8020093

Alarm	Attributes	Applicable major release
Name: IK8020093 (9200) Type: processingErrorAlarm Package: lmg.IK8020093 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-329 IK8020094

Alarm	Attributes	Applicable major release
Name: IK8020094 (9201) Type: processingErrorAlarm Package: lmg.IK8020094 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-330 IK8020095

Alarm	Attributes	Applicable major release
Name: IK8020095 (9202) Type: processingErrorAlarm Package: lmg.IK8020095 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-331 IK8020096

Alarm	Attributes	Applicable major release
Name: IK8020096 (9203) Type: processingErrorAlarm Package: lmg.IK8020096 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-332 IK8020097

Alarm	Attributes	Applicable major release
Name: IK8020097 (9204) Type: processingErrorAlarm Package: lmg.IK8020097 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-333 IK8020098

Alarm	Attributes	Applicable major release
Name: IK8020098 (9205) Type: processingErrorAlarm Package: lmg.IK8020098 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-334 IK8020099

Alarm	Attributes	Applicable major release
Name: IK8020099 (9206) Type: processingErrorAlarm Package: lmg.IK8020099 Raised on class: lmg.BpsFunction	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-335 IK8020100

Alarm	Attributes	Applicable major release
Name: IK8020100 (9723) Type: processingErrorAlarm Package: lmg.IK8020100 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-336 IK8020101

Alarm	Attributes	Applicable major release
Name: IK8020101 (9724) Type: processingErrorAlarm Package: lmg.IK8020101 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-337 IK8020102

Alarm	Attributes	Applicable major release
Name: IK8020102 (9725) Type: processingErrorAlarm Package: lmg.IK8020102 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-338 IK8020103

Alarm	Attributes	Applicable major release
Name: IK8020103 (9726) Type: processingErrorAlarm Package: Img.IK8020103 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-339 IK8020104

Alarm	Attributes	Applicable major release
Name: IK8020104 (9727) Type: processingErrorAlarm Package: Img.IK8020104 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-340 IK8020105

Alarm	Attributes	Applicable major release
Name: IK8020105 (9728) Type: processingErrorAlarm Package: Img.IK8020105 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-341 IK8020106

Alarm	Attributes	Applicable major release
Name: IK8020106 (9729) Type: processingErrorAlarm Package: Img.IK8020106 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-342 IK8020107

Alarm	Attributes	Applicable major release
Name: IK8020107 (9730) Type: processingErrorAlarm Package: lmg.IK8020107 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-343 IK8020108

Alarm	Attributes	Applicable major release
Name: IK8020108 (9731) Type: processingErrorAlarm Package: lmg.IK8020108 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-344 IK8020109

Alarm	Attributes	Applicable major release
Name: IK8020109 (9732) Type: processingErrorAlarm Package: lmg.IK8020109 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-345 IK8020110

Alarm	Attributes	Applicable major release
Name: IK8020110 (9733) Type: processingErrorAlarm Package: lmg.IK8020110 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-346 IK8020111

Alarm	Attributes	Applicable major release
Name: IK8020111 (9734) Type: processingErrorAlarm Package: Img.IK8020111 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-347 IK8020112

Alarm	Attributes	Applicable major release
Name: IK8020112 (9735) Type: processingErrorAlarm Package: Img.IK8020112 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-348 IK8020113

Alarm	Attributes	Applicable major release
Name: IK8020113 (9736) Type: processingErrorAlarm Package: Img.IK8020113 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-349 IK8020114

Alarm	Attributes	Applicable major release
Name: IK8020114 (9737) Type: processingErrorAlarm Package: Img.IK8020114 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-350 IK8020115

Alarm	Attributes	Applicable major release
Name: IK8020115 (9738) Type: processingErrorAlarm Package: lmg.IK8020115 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-351 IK8020116

Alarm	Attributes	Applicable major release
Name: IK8020116 (9739) Type: processingErrorAlarm Package: lmg.IK8020116 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-352 IK8020117

Alarm	Attributes	Applicable major release
Name: IK8020117 (9740) Type: processingErrorAlarm Package: lmg.IK8020117 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-353 IK8020118

Alarm	Attributes	Applicable major release
Name: IK8020118 (9741) Type: processingErrorAlarm Package: lmg.IK8020118 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-354 IK8020119

Alarm	Attributes	Applicable major release
Name: IK8020119 (9742) Type: processingErrorAlarm Package: Img.IK8020119 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-355 IK8020120

Alarm	Attributes	Applicable major release
Name: IK8020120 (9743) Type: processingErrorAlarm Package: Img.IK8020120 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-356 IK8020121

Alarm	Attributes	Applicable major release
Name: IK8020121 (9744) Type: processingErrorAlarm Package: Img.IK8020121 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-357 IK8020122

Alarm	Attributes	Applicable major release
Name: IK8020122 (9745) Type: processingErrorAlarm Package: Img.IK8020122 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-358 IK8020123

Alarm	Attributes	Applicable major release
Name: IK8020123 (9746) Type: processingErrorAlarm Package: Img.IK8020123 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-359 IK8020124

Alarm	Attributes	Applicable major release
Name: IK8020124 (9747) Type: processingErrorAlarm Package: Img.IK8020124 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-360 IK8020125

Alarm	Attributes	Applicable major release
Name: IK8020125 (9748) Type: processingErrorAlarm Package: Img.IK8020125 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-361 IK8020126

Alarm	Attributes	Applicable major release
Name: IK8020126 (9749) Type: processingErrorAlarm Package: Img.IK8020126 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-362 IK8020127

Alarm	Attributes	Applicable major release
Name: IK8020127 (9750) Type: processingErrorAlarm Package: Img.IK8020127 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-363 IK8020128

Alarm	Attributes	Applicable major release
Name: IK8020128 (9751) Type: processingErrorAlarm Package: Img.IK8020128 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-364 IK8020129

Alarm	Attributes	Applicable major release
Name: IK8020129 (9752) Type: processingErrorAlarm Package: Img.IK8020129 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-365 IK8020130

Alarm	Attributes	Applicable major release
Name: IK8020130 (9753) Type: processingErrorAlarm Package: Img.IK8020130 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-366 IK8020131

Alarm	Attributes	Applicable major release
Name: IK8020131 (9754) Type: processingErrorAlarm Package: lmg.IK8020131 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-367 IK8020132

Alarm	Attributes	Applicable major release
Name: IK8020132 (9755) Type: processingErrorAlarm Package: lmg.IK8020132 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-368 IK8020133

Alarm	Attributes	Applicable major release
Name: IK8020133 (9756) Type: processingErrorAlarm Package: lmg.IK8020133 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-369 IK8020134

Alarm	Attributes	Applicable major release
Name: IK8020134 (9757) Type: processingErrorAlarm Package: lmg.IK8020134 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-370 IK8020135

Alarm	Attributes	Applicable major release
Name: IK8020135 (9758) Type: processingErrorAlarm Package: Img.IK8020135 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-371 IK8020136

Alarm	Attributes	Applicable major release
Name: IK8020136 (9759) Type: processingErrorAlarm Package: Img.IK8020136 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-372 IK8020137

Alarm	Attributes	Applicable major release
Name: IK8020137 (9760) Type: processingErrorAlarm Package: Img.IK8020137 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-373 IK8020138

Alarm	Attributes	Applicable major release
Name: IK8020138 (9761) Type: processingErrorAlarm Package: Img.IK8020138 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-374 IK8020139

Alarm	Attributes	Applicable major release
Name: IK8020139 (9762) Type: processingErrorAlarm Package: lmg.IK8020139 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-375 IK8020140

Alarm	Attributes	Applicable major release
Name: IK8020140 (9763) Type: processingErrorAlarm Package: lmg.IK8020140 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-376 IK8020141

Alarm	Attributes	Applicable major release
Name: IK8020141 (9764) Type: processingErrorAlarm Package: lmg.IK8020141 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-377 IK8020142

Alarm	Attributes	Applicable major release
Name: IK8020142 (9765) Type: processingErrorAlarm Package: lmg.IK8020142 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-378 IK8020143

Alarm	Attributes	Applicable major release
Name: IK8020143 (9766) Type: processingErrorAlarm Package: Img.IK8020143 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-379 IK8020144

Alarm	Attributes	Applicable major release
Name: IK8020144 (9767) Type: processingErrorAlarm Package: Img.IK8020144 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-380 IK8020145

Alarm	Attributes	Applicable major release
Name: IK8020145 (9768) Type: processingErrorAlarm Package: Img.IK8020145 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-381 IK8020146

Alarm	Attributes	Applicable major release
Name: IK8020146 (9769) Type: processingErrorAlarm Package: Img.IK8020146 Raised on class: Img.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-382 IK8020147

Alarm	Attributes	Applicable major release
Name: IK8020147 (9770) Type: processingErrorAlarm Package: lmg.IK8020147 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-383 IK8020148

Alarm	Attributes	Applicable major release
Name: IK8020148 (9771) Type: processingErrorAlarm Package: lmg.IK8020148 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-384 IK8020149

Alarm	Attributes	Applicable major release
Name: IK8020149 (9772) Type: processingErrorAlarm Package: lmg.IK8020149 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-385 IK8020201

Alarm	Attributes	Applicable major release
Name: IK8020201 (10319) Type: processingErrorAlarm Package: lmg.IK8020201 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Session state discrepancy Implicitly cleared: true Default probable cause: databaseInconsistency	Release: • LR16.1.MG
Description: This event is raised when BPS discovers session state discrepancy at a BMSC\nReason: Session state discrepancy		
Remedial action: No action is required.		

Table 27-386 IK8020205

Alarm	Attributes	Applicable major release
Name: IK8020205 (9774) Type: communicationsAlarm Package: lmg.IK8020205 Raised on class: lmg.BpsFunction	Severity: indeterminate Specific problem: Unauthorized BPS REST interface access Implicitly cleared: true Default probable cause: invalidMessageReceived	Release: • LR16.1.MG
Description: This event is raised when BPS detects unauthorized access to the REST interface\nReason: Unauthorized BPS REST interface access		
Remedial action: No action is required.		

Table 27-387 IK8020230

Alarm	Attributes	Applicable major release
Name: IK8020230 (10320) Type: qualityOfServiceAlarm Package: lmg.IK8020230 Raised on class: lmg.BpsFunction	Severity: minor Specific problem: eMBMS session not admitted Implicitly cleared: true Default probable cause: systemResourcesOverload	Release: • LR16.1.MG
Description: This alarm is raised when a MCE failed to admit an eMBMS session. Alarm is cleared by the system.\nReason: eMBMS session not admitted		
Remedial action: Operator should investigate potential impact to session quality		

Table 27-388 IK8100004

Alarm	Attributes	Applicable major release
Name: IK8100004 (6465) Type: communicationsAlarm Package: lmg.IK8100004 Raised on class: lmg.GSEM	Severity: critical Specific problem: GSEM cannot interrogate this equipment Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is raised when there is a problem in the procedure and/or process that requires conveying information from one point to another. Alarm is cleared by the system.\nReason: GSEM cannot interrogate this equipment		
Remedial action: Check the equipment status and the GSEM/NE connection		

Table 27-389 IK8100005

Alarm	Attributes	Applicable major release
Name: IK8100005 (6466) Type: processingErrorAlarm Package: lmg.IK8100005 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Monitored object status change Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: a configurable string is displayed. Alarm is cleared by the system.\nReason: Monitored object status change		
Remedial action: Check the object		

Table 27-390 IK8100006

Alarm	Attributes	Applicable major release
Name: IK8100006 (6467) Type: processingErrorAlarm Package: lmg.IK8100006 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Change of consolidated status of a submap Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Map Name and new status are displayed. Alarm is cleared by the system.\nReason: Map Status Change		
Remedial action: Check the submap		

Table 27-391 IK8100007

Alarm	Attributes	Applicable major release
Name: IK8100007 (6468) Type: processingErrorAlarm Package: lmg.IK8100007 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Change of Icon status Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Icon Name and status change reason are displayed. Alarm is cleared by the system.\nReason: Icon Status Change		
Remedial action: Check the object attached to the icon		

Table 27-392 IK8100046

Alarm	Attributes	Applicable major release
Name: IK8100046 (6469) Type: processingErrorAlarm Package: lmg.IK8100046 Raised on class: lmg.GSEM	Severity: warning Specific problem: GSEM starts Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-392 IK8100046 (continued)

Alarm	Attributes	Applicable major release
Description: Security log for different cases, see alarm content to know which case is encountered. The alarm is managed through the Auto-Clear feature so that it is cleared automatically by the system after a delay.\nReason: Add equipment , Apply Configuration, Authorization created, Authorization deleted, Authorization modified, Auto-load Map, AutoLoad Map added, AutoLoad Map removed, Automatic Account Unlock, Automatic History Purge, Automatic Pending Event Purge, Automatic Restart after connection loss, Cannot apply configuration, Cannot register as alarm destination, Cut-through activated, Delete equipment, Event Processing configuration created, Event Processing configuration deleted, Event Processing configuration modified, Event Processing configuration saved, File export, File Lookup Load, File transfer error, Filter deleted, Filter saved, Light Client connected, Light Client disconnected, Light Client ejected, Log File Received, Login failure, Map FAD updated, Modify equipment, NAD created, NAD deleted, NAD modified, NeReporterPlugin modified, No free row to register as alarm destination, Object Locked, Object Unlocked, Password modified, Perf polling started, Perf polling stopped, Remote User login, Remote User login Failure, Remote User logout, Server shutdown, Server startup, Starting plugin, StatsPlugin modified, User Account Locked, User Account UnLocked, User Ejected, User list modified, User login, User logout Reason:Add equipment , Apply Configuration, Authorization created, Authorization deleted, Authorization modified, Auto-load Map, AutoLoad Map added, AutoLoad Map removed, Automatic Account Unlock, Automatic History Purge, Automatic Pending Event Purge, Automatic Restart after connection loss, Cannot apply configuration, Cannot register as alarm destination, Cut-through activated, Delete equipment, Event Processing configuration created, Event Processing configuration deleted, Event Processing configuration modified, Event Processing configuration saved, File export, File Lookup Load, File transfer error, Filter deleted, Filter saved, Light Client connected, Light Client disconnected, Light Client ejected, Log File Received, Login failure, Map FAD updated, Modify equipment, NAD created, NAD deleted, NAD modified, NeReporterPlugin modified, No free row to register as alarm destination, Object Locked, Object Unlocked, Password modified, Perf polling started, Perf polling stopped, Remote User ...		
Remedial action: Check GSEM alarm content		

Table 27-393 IK8100068

Alarm	Attributes	Applicable major release
Name: IK8100068 (6470) Type: processingErrorAlarm Package: Img.IK8100068 Raised on class: Img.GSEM	Severity: major Specific problem: Information - GSEM Server Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The GSEM server licence will expire - the date information is available on GSEM alarm. Alarm is cleared by the system when the service is restarted.\nReason: Licence trap		
Remedial action: Check the date, order a licence		

Table 27-394 IK8100075

Alarm	Attributes	Applicable major release
Name: IK8100075 (9207) Type: processingErrorAlarm Package: Img.IK8100075 Raised on class: Img.GSEM	Severity: warning Specific problem: Self care information - perf data directory Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Self care information - perf data directory. Alarm is cleared by the system.\nReason: Perf Data Size Overflow		
Remedial action: Check the configured perf directory (by default /space/GSEM/Server/Main/etc/data/Perf/[ne_type])>		

Table 27-395 IK8100076

Alarm	Attributes	Applicable major release
Name: IK8100076 (6471) Type: processingErrorAlarm Package: lmg.IK8100076 Raised on class: lmg.GSEM	Severity: warning Specific problem: Self care information -graph data directory Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Self care information -graph data directory. Alarm is cleared by the system.\nReason: Graph Data Size Overflow		
Remedial action: Check the configured graph data directory (by default /space/GSEM/Server/Main/etc/graphData)		

Table 27-396 IK8100077

Alarm	Attributes	Applicable major release
Name: IK8100077 (6472) Type: processingErrorAlarm Package: lmg.IK8100077 Raised on class: lmg.GSEM	Severity: warning Specific problem: Self care information - log directory Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Self care information - log directory. Alarm is cleared by the system.\nReason: Log Data Size Overflow		
Remedial action: Check the log directory (by default /space/GSEM/Server/Main/etc/log)		

Table 27-397 IK8100080

Alarm	Attributes	Applicable major release
Name: IK8100080 (9208) Type: communicationsAlarm Package: lmg.IK8100080 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: SAM-GSEM-LMGOAM interface issue Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm is raised in case of LMG interface issue for Inventory or conf. Mgt files (e. G. LMG node name/version, LMG inventory file cannot be retrieved, or configuration operation failure). See detailed cause in the alarm.. Alarm is cleared by the system.\nReason: Get LMG Node name and version, Get LMG Inventory file version, Get Inventory file: failure, Configuration operation request, Configuration operation partially failed in LMGOaM, Configuration operation failed in LMGOaM		
Remedial action: Check configuration		

Table 27-398 IK8100081

Alarm	Attributes	Applicable major release
Name: IK8100081 (10321) Type: processingErrorAlarm Package: lmg.IK8100081 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Debouncing statistics Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This event is raised in case of LMG alarm bouncing. AlarmId of the transient alarm, and occurences number is indicated in the trap\nReason: Transient LMG alarms		
Remedial action: No action is required.		

Table 27-399 IK8100104

Alarm	Attributes	Applicable major release
Name: IK8100104 (10322) Type: communicationsAlarm Package: lmg.IK8100104 Raised on class: lmg.FRU	Severity: critical Specific problem: GSEM cannot interrogate this equipment Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm is raised when there is a problem in the procedure and/or process that requires conveying information from one point to another. Alarm is cleared by the system.\nReason: Communication problem with equipment		
Remedial action: Check the equipment status and the GSEM/NE connection		

Table 27-400 IK8100105

Alarm	Attributes	Applicable major release
Name: IK8100105 (10323) Type: processingErrorAlarm Package: lmg.IK8100105 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Monitored object status change Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: a configurable string is displayed. Alarm is cleared by the system.\nReason: Monitoring		
Remedial action: Check the object		

Table 27-401 IK8100500

Alarm	Attributes	Applicable major release
Name: IK8100500 (9209) Type: processingErrorAlarm Package: lmg.IK8100500 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-402 IK8100501

Alarm	Attributes	Applicable major release
Name: IK8100501 (9210) Type: processingErrorAlarm Package: lmg.IK8100501 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-403 IK8100502

Alarm	Attributes	Applicable major release
Name: IK8100502 (9211) Type: processingErrorAlarm Package: lmg.IK8100502 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-404 IK8100503

Alarm	Attributes	Applicable major release
Name: IK8100503 (9212) Type: processingErrorAlarm Package: lmg.IK8100503 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-405 IK8100504

Alarm	Attributes	Applicable major release
Name: IK8100504 (9213) Type: processingErrorAlarm Package: Img.IK8100504 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-406 IK8100505

Alarm	Attributes	Applicable major release
Name: IK8100505 (9214) Type: processingErrorAlarm Package: Img.IK8100505 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-407 IK8100506

Alarm	Attributes	Applicable major release
Name: IK8100506 (9215) Type: processingErrorAlarm Package: Img.IK8100506 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-408 IK8100507

Alarm	Attributes	Applicable major release
Name: IK8100507 (9216) Type: processingErrorAlarm Package: Img.IK8100507 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-409 IK8100508

Alarm	Attributes	Applicable major release
Name: IK8100508 (9217) Type: processingErrorAlarm Package: lmg.IK8100508 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-410 IK8100509

Alarm	Attributes	Applicable major release
Name: IK8100509 (9218) Type: processingErrorAlarm Package: lmg.IK8100509 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-411 IK8100510

Alarm	Attributes	Applicable major release
Name: IK8100510 (9219) Type: processingErrorAlarm Package: lmg.IK8100510 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-412 IK8100511

Alarm	Attributes	Applicable major release
Name: IK8100511 (9220) Type: processingErrorAlarm Package: lmg.IK8100511 Raised on class: lmg.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-413 IK8100512

Alarm	Attributes	Applicable major release
Name: IK8100512 (9221) Type: processingErrorAlarm Package: Img.IK8100512 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-414 IK8100513

Alarm	Attributes	Applicable major release
Name: IK8100513 (9222) Type: processingErrorAlarm Package: Img.IK8100513 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-415 IK8100514

Alarm	Attributes	Applicable major release
Name: IK8100514 (9223) Type: processingErrorAlarm Package: Img.IK8100514 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-416 IK8100515

Alarm	Attributes	Applicable major release
Name: IK8100515 (9224) Type: processingErrorAlarm Package: Img.IK8100515 Raised on class: Img.GSEM	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-417 IK8100520

Alarm	Attributes	Applicable major release
Name: IK8100520 (9775) Type: processingErrorAlarm Package: Img.IK8100520 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-418 IK8100521

Alarm	Attributes	Applicable major release
Name: IK8100521 (9776) Type: processingErrorAlarm Package: Img.IK8100521 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-419 IK8100522

Alarm	Attributes	Applicable major release
Name: IK8100522 (9777) Type: processingErrorAlarm Package: Img.IK8100522 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-420 IK8100523

Alarm	Attributes	Applicable major release
Name: IK8100523 (9778) Type: processingErrorAlarm Package: Img.IK8100523 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-421 IK8100524

Alarm	Attributes	Applicable major release
Name: IK8100524 (9779) Type: processingErrorAlarm Package: Img.IK8100524 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-422 IK8100525

Alarm	Attributes	Applicable major release
Name: IK8100525 (9780) Type: processingErrorAlarm Package: Img.IK8100525 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-423 IK8100526

Alarm	Attributes	Applicable major release
Name: IK8100526 (9781) Type: processingErrorAlarm Package: Img.IK8100526 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-424 IK8100527

Alarm	Attributes	Applicable major release
Name: IK8100527 (9782) Type: processingErrorAlarm Package: Img.IK8100527 Raised on class: Img.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-425 IK8100528

Alarm	Attributes	Applicable major release
Name: IK8100528 (9783) Type: processingErrorAlarm Package: lmg.IK8100528 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-426 IK8100529

Alarm	Attributes	Applicable major release
Name: IK8100529 (9784) Type: processingErrorAlarm Package: lmg.IK8100529 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-427 IK8100530

Alarm	Attributes	Applicable major release
Name: IK8100530 (9785) Type: processingErrorAlarm Package: lmg.IK8100530 Raised on class: lmg.GSEM	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-428 IK8200982

Alarm	Attributes	Applicable major release
Name: IK8200982 (6473) Type: equipmentAlarm Package: lmg.IK8200982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-429 IK8200984

Alarm	Attributes	Applicable major release
Name: IK8200984 (6474) Type: processingErrorAlarm Package: Img.IK8200984 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-430 IK8200986

Alarm	Attributes	Applicable major release
Name: IK8200986 (6475) Type: equipmentAlarm Package: Img.IK8200986 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-431 IK8201008

Alarm	Attributes	Applicable major release
Name: IK8201008 (6476) Type: equipmentAlarm Package: Img.IK8201008 Raised on class: Img.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-432 IK8201010

Alarm	Attributes	Applicable major release
Name: IK8201010 (6477) Type: equipmentAlarm Package: lmg.IK8201010 Raised on class: lmg.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-433 IK8201013

Alarm	Attributes	Applicable major release
Name: IK8201013 (6478) Type: equipmentAlarm Package: lmg.IK8201013 Raised on class: lmg.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-434 IK8201018

Alarm	Attributes	Applicable major release
Name: IK8201018 (6479) Type: processingErrorAlarm Package: lmg.IK8201018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-435 IK8201023

Alarm	Attributes	Applicable major release
Name: IK8201023 (6480) Type: processingErrorAlarm Package: lmg.IK8201023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-435 IK8201023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-436 IK8201030

Alarm	Attributes	Applicable major release
Name: IK8201030 (6481) Type: equipmentAlarm Package: lmg.IK8201030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-437 IK8201033

Alarm	Attributes	Applicable major release
Name: IK8201033 (6482) Type: equipmentAlarm Package: lmg.IK8201033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-438 IK8201037

Alarm	Attributes	Applicable major release
Name: IK8201037 (6483) Type: equipmentAlarm Package: lmg.IK8201037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		

Table 27-438 IK8201037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-439 IK8201040

Alarm	Attributes	Applicable major release
Name: IK8201040 (6484) Type: environmentalAlarm Package: lmg.IK8201040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-440 IK8201060

Alarm	Attributes	Applicable major release
Name: IK8201060 (6485) Type: environmentalAlarm Package: lmg.IK8201060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-441 IK8201073

Alarm	Attributes	Applicable major release
Name: IK8201073 (6486) Type: environmentalAlarm Package: lmg.IK8201073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		

Table 27-441 IK8201073 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the Accelerator Cache Board.		

Table 27-442 IK8201091

Alarm	Attributes	Applicable major release
Name: IK8201091 (9225) Type: environmentalAlarm Package: Img.IK8201091 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-443 IK8201098

Alarm	Attributes	Applicable major release
Name: IK8201098 (6487) Type: equipmentAlarm Package: Img.IK8201098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-444 IK8201102

Alarm	Attributes	Applicable major release
Name: IK8201102 (6488) Type: environmentalAlarm Package: Img.IK8201102 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-445 IK8201105

Alarm	Attributes	Applicable major release
Name: IK8201105 (6489) Type: environmentalAlarm Package: Img.IK8201105 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-446 IK8201112

Alarm	Attributes	Applicable major release
Name: IK8201112 (6490) Type: equipmentAlarm Package: Img.IK8201112 Raised on class: Img.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-447 IK8201116

Alarm	Attributes	Applicable major release
Name: IK8201116 (6491) Type: equipmentAlarm Package: Img.IK8201116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-448 IK8201121

Alarm	Attributes	Applicable major release
Name: IK8201121 (6492) Type: environmentalAlarm Package: Img.IK8201121 Raised on class: Img.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-449 IK8201125

Alarm	Attributes	Applicable major release
Name: IK8201125 (6493) Type: environmentalAlarm Package: Img.IK8201125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-450 IK8201129

Alarm	Attributes	Applicable major release
Name: IK8201129 (6494) Type: equipmentAlarm Package: Img.IK8201129 Raised on class: Img.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-451 IK8201135

Alarm	Attributes	Applicable major release
Name: IK8201135 (6495) Type: equipmentAlarm Package: Img.IK8201135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-451 IK8201135 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-452 IK8201144

Alarm	Attributes	Applicable major release
Name: IK8201144 (6496) Type: processingErrorAlarm Package: lmg.IK8201144 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-453 IK8201148

Alarm	Attributes	Applicable major release
Name: IK8201148 (6497) Type: equipmentAlarm Package: lmg.IK8201148 Raised on class: lmg.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-454 IK8201152

Alarm	Attributes	Applicable major release
Name: IK8201152 (6498) Type: processingErrorAlarm Package: lmg.IK8201152 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		

Table 27-454 IK8201152 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-455 IK8201154

Alarm	Attributes	Applicable major release
Name: IK8201154 (6499) Type: equipmentAlarm Package: lmg.IK8201154 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-456 IK8201156

Alarm	Attributes	Applicable major release
Name: IK8201156 (6500) Type: processingErrorAlarm Package: lmg.IK8201156 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-457 IK8201158

Alarm	Attributes	Applicable major release
Name: IK8201158 (6501) Type: processingErrorAlarm Package: lmg.IK8201158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-458 IK8201160

Alarm	Attributes	Applicable major release
Name: IK8201160 (9226) Type: communicationsAlarm Package: lmg.IK8201160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-459 IK8201163

Alarm	Attributes	Applicable major release
Name: IK8201163 (6502) Type: communicationsAlarm Package: lmg.IK8201163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-460 IK8201172

Alarm	Attributes	Applicable major release
Name: IK8201172 (6503) Type: qualityOfServiceAlarm Package: lmg.IK8201172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-461 IK8202265

Alarm	Attributes	Applicable major release
Name: IK8202265 (6504) Type: environmentalAlarm Package: Img.IK8202265 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-462 IK8202272

Alarm	Attributes	Applicable major release
Name: IK8202272 (6505) Type: environmentalAlarm Package: Img.IK8202272 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-463 IK8202279

Alarm	Attributes	Applicable major release
Name: IK8202279 (6506) Type: environmentalAlarm Package: Img.IK8202279 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-464 IK8202291

Alarm	Attributes	Applicable major release
Name: IK8202291 (6507) Type: equipmentAlarm Package: lmg.IK8202291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-465 IK8202292

Alarm	Attributes	Applicable major release
Name: IK8202292 (6508) Type: environmentalAlarm Package: lmg.IK8202292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-466 IK8202295

Alarm	Attributes	Applicable major release
Name: IK8202295 (6509) Type: equipmentAlarm Package: lmg.IK8202295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-467 IK8202302

Alarm	Attributes	Applicable major release
Name: IK8202302 (6510) Type: equipmentAlarm Package: Img.IK8202302 Raised on class: Img.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-468 IK8202337

Alarm	Attributes	Applicable major release
Name: IK8202337 (6511) Type: communicationsAlarm Package: Img.IK8202337 Raised on class: Img.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-469 IK8202341

Alarm	Attributes	Applicable major release
Name: IK8202341 (6512) Type: communicationsAlarm Package: Img.IK8202341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-470 IK8202343

Alarm	Attributes	Applicable major release
Name: IK8202343 (6513) Type: communicationsAlarm Package: lmg.IK8202343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-471 IK8202347

Alarm	Attributes	Applicable major release
Name: IK8202347 (6514) Type: communicationsAlarm Package: lmg.IK8202347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-472 IK8202349

Alarm	Attributes	Applicable major release
Name: IK8202349 (6515) Type: communicationsAlarm Package: lmg.IK8202349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-473 IK8202360

Alarm	Attributes	Applicable major release
Name: IK8202360 (6516) Type: equipmentAlarm Package: Img.IK8202360 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-474 IK8202363

Alarm	Attributes	Applicable major release
Name: IK8202363 (6517) Type: environmentalAlarm Package: Img.IK8202363 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-475 IK8202368

Alarm	Attributes	Applicable major release
Name: IK8202368 (6518) Type: equipmentAlarm Package: Img.IK8202368 Raised on class: Img.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-476 IK8202369

Alarm	Attributes	Applicable major release
Name: IK8202369 (6519) Type: equipmentAlarm Package: lmg.IK8202369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-477 IK8202374

Alarm	Attributes	Applicable major release
Name: IK8202374 (6520) Type: equipmentAlarm Package: lmg.IK8202374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-478 IK8202375

Alarm	Attributes	Applicable major release
Name: IK8202375 (6521) Type: equipmentAlarm Package: lmg.IK8202375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-479 IK8202376

Alarm	Attributes	Applicable major release
Name: IK8202376 (6522) Type: equipmentAlarm Package: Img.IK8202376 Raised on class: Img.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-480 IK8202377

Alarm	Attributes	Applicable major release
Name: IK8202377 (6523) Type: equipmentAlarm Package: Img.IK8202377 Raised on class: Img.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-481 IK8202378

Alarm	Attributes	Applicable major release
Name: IK8202378 (6524) Type: equipmentAlarm Package: Img.IK8202378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-482 IK8202379

Alarm	Attributes	Applicable major release
Name: IK8202379 (6525) Type: equipmentAlarm Package: Img.IK8202379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-483 IK8202380

Alarm	Attributes	Applicable major release
Name: IK8202380 (6526) Type: equipmentAlarm Package: Img.IK8202380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-484 IK8202382

Alarm	Attributes	Applicable major release
Name: IK8202382 (6527) Type: environmentalAlarm Package: Img.IK8202382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-485 IK8202386

Alarm	Attributes	Applicable major release
Name: IK8202386 (6528) Type: equipmentAlarm Package: Img.IK8202386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-486 IK8202387

Alarm	Attributes	Applicable major release
Name: IK8202387 (6529) Type: equipmentAlarm Package: Img.IK8202387 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-487 IK8202388

Alarm	Attributes	Applicable major release
Name: IK8202388 (6530) Type: equipmentAlarm Package: Img.IK8202388 Raised on class: Img.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-488 IK8202391

Alarm	Attributes	Applicable major release
Name: IK8202391 (6531) Type: processingErrorAlarm Package: lmg.IK8202391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-489 IK8202401

Alarm	Attributes	Applicable major release
Name: IK8202401 (6532) Type: communicationsAlarm Package: lmg.IK8202401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-490 IK8202408

Alarm	Attributes	Applicable major release
Name: IK8202408 (6533) Type: qualityOfServiceAlarm Package: lmg.IK8202408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-491 IK8202409

Alarm	Attributes	Applicable major release
Name: IK8202409 (6534) Type: processingErrorAlarm Package: Img.IK8202409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-492 IK8202411

Alarm	Attributes	Applicable major release
Name: IK8202411 (6535) Type: equipmentAlarm Package: Img.IK8202411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-493 IK8202428

Alarm	Attributes	Applicable major release
Name: IK8202428 (6536) Type: equipmentAlarm Package: Img.IK8202428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-494 IK8202429

Alarm	Attributes	Applicable major release
Name: IK8202429 (6537) Type: equipmentAlarm Package: Img.IK8202429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		

Table 27-494 IK8202429 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-495 IK8202431

Alarm	Attributes	Applicable major release
Name: IK8202431 (6538) Type: equipmentAlarm Package: lmg.IK8202431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-496 IK8202432

Alarm	Attributes	Applicable major release
Name: IK8202432 (6539) Type: equipmentAlarm Package: lmg.IK8202432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-497 IK8202436

Alarm	Attributes	Applicable major release
Name: IK8202436 (6540) Type: equipmentAlarm Package: lmg.IK8202436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-498 IK8202437

Alarm	Attributes	Applicable major release
Name: IK8202437 (6541) Type: equipmentAlarm Package: lmg.IK8202437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-499 IK8202439

Alarm	Attributes	Applicable major release
Name: IK8202439 (6542) Type: communicationsAlarm Package: lmg.IK8202439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-500 IK8202559

Alarm	Attributes	Applicable major release
Name: IK8202559 (6543) Type: equipmentAlarm Package: lmg.IK8202559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-501 IK8202609

Alarm	Attributes	Applicable major release
Name: IK8202609 (6544) Type: processingErrorAlarm Package: lmg.IK8202609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-501 IK8202609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-502 IK8202610

Alarm	Attributes	Applicable major release
Name: IK8202610 (6545) Type: processingErrorAlarm Package: lmg.IK8202610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-503 IK8202615

Alarm	Attributes	Applicable major release
Name: IK8202615 (6546) Type: equipmentAlarm Package: lmg.IK8202615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-504 IK8202616

Alarm	Attributes	Applicable major release
Name: IK8202616 (6547) Type: environmentalAlarm Package: Img.IK8202616 Raised on class: Img.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-505 IK8202617

Alarm	Attributes	Applicable major release
Name: IK8202617 (6548) Type: environmentalAlarm Package: Img.IK8202617 Raised on class: Img.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-506 IK8202620

Alarm	Attributes	Applicable major release
Name: IK8202620 (6549) Type: equipmentAlarm Package: Img.IK8202620 Raised on class: Img.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-507 IK8202622

Alarm	Attributes	Applicable major release
Name: IK8202622 (6550) Type: environmentalAlarm Package: Img.IK8202622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-508 IK8202628

Alarm	Attributes	Applicable major release
Name: IK8202628 (6551) Type: equipmentAlarm Package: Img.IK8202628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-509 IK8202632

Alarm	Attributes	Applicable major release
Name: IK8202632 (6552) Type: processingErrorAlarm Package: Img.IK8202632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-510 IK8202633

Alarm	Attributes	Applicable major release
Name: IK8202633 (6553) Type: communicationsAlarm Package: Img.IK8202633 Raised on class: Img.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-511 IK8202636

Alarm	Attributes	Applicable major release
Name: IK8202636 (9227) Type: equipmentAlarm Package: Img.IK8202636 Raised on class: Img.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-512 IK8202648

Alarm	Attributes	Applicable major release
Name: IK8202648 (6554) Type: qualityOfServiceAlarm Package: Img.IK8202648 Raised on class: Img.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-513 IK8202657

Alarm	Attributes	Applicable major release
Name: IK8202657 (6555) Type: environmentalAlarm Package: lmg.IK8202657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-514 IK8204762

Alarm	Attributes	Applicable major release
Name: IK8204762 (6556) Type: communicationsAlarm Package: lmg.IK8204762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-515 IK8250982

Alarm	Attributes	Applicable major release
Name: IK8250982 (6557) Type: equipmentAlarm Package: lmg.IK8250982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-516 IK8250984

Alarm	Attributes	Applicable major release
Name: IK8250984 (6558) Type: processingErrorAlarm Package: Img.IK8250984 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-517 IK8250986

Alarm	Attributes	Applicable major release
Name: IK8250986 (6559) Type: equipmentAlarm Package: Img.IK8250986 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-518 IK8251008

Alarm	Attributes	Applicable major release
Name: IK8251008 (6560) Type: equipmentAlarm Package: Img.IK8251008 Raised on class: Img.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-519 IK8251010

Alarm	Attributes	Applicable major release
Name: IK8251010 (6561) Type: equipmentAlarm Package: lmg.IK8251010 Raised on class: lmg.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-520 IK8251013

Alarm	Attributes	Applicable major release
Name: IK8251013 (6562) Type: equipmentAlarm Package: lmg.IK8251013 Raised on class: lmg.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-521 IK8251018

Alarm	Attributes	Applicable major release
Name: IK8251018 (6563) Type: processingErrorAlarm Package: lmg.IK8251018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-522 IK8251023

Alarm	Attributes	Applicable major release
Name: IK8251023 (6564) Type: processingErrorAlarm Package: lmg.IK8251023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-522 IK8251023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-523 IK8251030

Alarm	Attributes	Applicable major release
Name: IK8251030 (6565) Type: equipmentAlarm Package: Img.IK8251030 Raised on class: Img.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-524 IK8251033

Alarm	Attributes	Applicable major release
Name: IK8251033 (6566) Type: equipmentAlarm Package: Img.IK8251033 Raised on class: Img.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-525 IK8251037

Alarm	Attributes	Applicable major release
Name: IK8251037 (6567) Type: equipmentAlarm Package: Img.IK8251037 Raised on class: Img.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		

Table 27-525 IK8251037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-526 IK8251040

Alarm	Attributes	Applicable major release
Name: IK8251040 (6568) Type: environmentalAlarm Package: lmg.IK8251040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-527 IK8251060

Alarm	Attributes	Applicable major release
Name: IK8251060 (6569) Type: environmentalAlarm Package: lmg.IK8251060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-528 IK8251073

Alarm	Attributes	Applicable major release
Name: IK8251073 (6570) Type: environmentalAlarm Package: lmg.IK8251073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		

Table 27-528 IK8251073 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the Accelerator Cache Board.		

Table 27-529 IK8251091

Alarm	Attributes	Applicable major release
Name: IK8251091 (9228) Type: environmentalAlarm Package: Img.IK8251091 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-530 IK8251098

Alarm	Attributes	Applicable major release
Name: IK8251098 (6571) Type: equipmentAlarm Package: Img.IK8251098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-531 IK8251102

Alarm	Attributes	Applicable major release
Name: IK8251102 (6572) Type: environmentalAlarm Package: Img.IK8251102 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-532 IK8251105

Alarm	Attributes	Applicable major release
Name: IK8251105 (6573) Type: environmentalAlarm Package: Img.IK8251105 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-533 IK8251112

Alarm	Attributes	Applicable major release
Name: IK8251112 (6574) Type: equipmentAlarm Package: Img.IK8251112 Raised on class: Img.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-534 IK8251116

Alarm	Attributes	Applicable major release
Name: IK8251116 (6575) Type: equipmentAlarm Package: Img.IK8251116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-535 IK8251121

Alarm	Attributes	Applicable major release
Name: IK8251121 (6576) Type: environmentalAlarm Package: Img.IK8251121 Raised on class: Img.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-536 IK8251125

Alarm	Attributes	Applicable major release
Name: IK8251125 (6577) Type: environmentalAlarm Package: Img.IK8251125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-537 IK8251129

Alarm	Attributes	Applicable major release
Name: IK8251129 (6578) Type: equipmentAlarm Package: Img.IK8251129 Raised on class: Img.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-538 IK8251135

Alarm	Attributes	Applicable major release
Name: IK8251135 (6579) Type: equipmentAlarm Package: Img.IK8251135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-538 IK8251135 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-539 IK8251144

Alarm	Attributes	Applicable major release
Name: IK8251144 (6580) Type: processingErrorAlarm Package: Img.IK8251144 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-540 IK8251148

Alarm	Attributes	Applicable major release
Name: IK8251148 (6581) Type: equipmentAlarm Package: Img.IK8251148 Raised on class: Img.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-541 IK8251152

Alarm	Attributes	Applicable major release
Name: IK8251152 (6582) Type: processingErrorAlarm Package: Img.IK8251152 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		

Table 27-541 IK8251152 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-542 IK8251154

Alarm	Attributes	Applicable major release
Name: IK8251154 (6583) Type: equipmentAlarm Package: Img.IK8251154 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-543 IK8251156

Alarm	Attributes	Applicable major release
Name: IK8251156 (6584) Type: processingErrorAlarm Package: Img.IK8251156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-544 IK8251158

Alarm	Attributes	Applicable major release
Name: IK8251158 (6585) Type: processingErrorAlarm Package: Img.IK8251158 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-545 IK8251160

Alarm	Attributes	Applicable major release
Name: IK8251160 (9229) Type: communicationsAlarm Package: lmg.IK8251160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-546 IK8251163

Alarm	Attributes	Applicable major release
Name: IK8251163 (6586) Type: communicationsAlarm Package: lmg.IK8251163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-547 IK8251172

Alarm	Attributes	Applicable major release
Name: IK8251172 (6587) Type: qualityOfServiceAlarm Package: lmg.IK8251172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-548 IK8252265

Alarm	Attributes	Applicable major release
Name: IK8252265 (6588) Type: environmentalAlarm Package: lmg.IK8252265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-549 IK8252272

Alarm	Attributes	Applicable major release
Name: IK8252272 (6589) Type: environmentalAlarm Package: lmg.IK8252272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-550 IK8252279

Alarm	Attributes	Applicable major release
Name: IK8252279 (6590) Type: environmentalAlarm Package: lmg.IK8252279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-551 IK8252291

Alarm	Attributes	Applicable major release
Name: IK8252291 (6591) Type: equipmentAlarm Package: lmg.IK8252291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-552 IK8252292

Alarm	Attributes	Applicable major release
Name: IK8252292 (6592) Type: environmentalAlarm Package: lmg.IK8252292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-553 IK8252295

Alarm	Attributes	Applicable major release
Name: IK8252295 (6593) Type: equipmentAlarm Package: lmg.IK8252295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-554 IK8252302

Alarm	Attributes	Applicable major release
Name: IK8252302 (6594) Type: equipmentAlarm Package: Img.IK8252302 Raised on class: Img.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-555 IK8252337

Alarm	Attributes	Applicable major release
Name: IK8252337 (6595) Type: communicationsAlarm Package: Img.IK8252337 Raised on class: Img.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-556 IK8252341

Alarm	Attributes	Applicable major release
Name: IK8252341 (6596) Type: communicationsAlarm Package: Img.IK8252341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-557 IK8252343

Alarm	Attributes	Applicable major release
Name: IK8252343 (6597) Type: communicationsAlarm Package: lmg.IK8252343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-558 IK8252347

Alarm	Attributes	Applicable major release
Name: IK8252347 (6598) Type: communicationsAlarm Package: lmg.IK8252347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-559 IK8252349

Alarm	Attributes	Applicable major release
Name: IK8252349 (6599) Type: communicationsAlarm Package: lmg.IK8252349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-560 IK8252360

Alarm	Attributes	Applicable major release
Name: IK8252360 (6600) Type: equipmentAlarm Package: Img.IK8252360 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-561 IK8252363

Alarm	Attributes	Applicable major release
Name: IK8252363 (6601) Type: environmentalAlarm Package: Img.IK8252363 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-562 IK8252368

Alarm	Attributes	Applicable major release
Name: IK8252368 (6602) Type: equipmentAlarm Package: Img.IK8252368 Raised on class: Img.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-563 IK8252369

Alarm	Attributes	Applicable major release
Name: IK8252369 (6603) Type: equipmentAlarm Package: lmg.IK8252369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-564 IK8252374

Alarm	Attributes	Applicable major release
Name: IK8252374 (6604) Type: equipmentAlarm Package: lmg.IK8252374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-565 IK8252375

Alarm	Attributes	Applicable major release
Name: IK8252375 (6605) Type: equipmentAlarm Package: lmg.IK8252375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-566 IK8252376

Alarm	Attributes	Applicable major release
Name: IK8252376 (6606) Type: equipmentAlarm Package: Img.IK8252376 Raised on class: Img.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-567 IK8252377

Alarm	Attributes	Applicable major release
Name: IK8252377 (6607) Type: equipmentAlarm Package: Img.IK8252377 Raised on class: Img.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-568 IK8252378

Alarm	Attributes	Applicable major release
Name: IK8252378 (6608) Type: equipmentAlarm Package: Img.IK8252378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-569 IK8252379

Alarm	Attributes	Applicable major release
Name: IK8252379 (6609) Type: equipmentAlarm Package: Img.IK8252379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-570 IK8252380

Alarm	Attributes	Applicable major release
Name: IK8252380 (6610) Type: equipmentAlarm Package: Img.IK8252380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-571 IK8252382

Alarm	Attributes	Applicable major release
Name: IK8252382 (6611) Type: environmentalAlarm Package: Img.IK8252382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-572 IK8252386

Alarm	Attributes	Applicable major release
Name: IK8252386 (6612) Type: equipmentAlarm Package: Img.IK8252386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-573 IK8252387

Alarm	Attributes	Applicable major release
Name: IK8252387 (6613) Type: equipmentAlarm Package: Img.IK8252387 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-574 IK8252388

Alarm	Attributes	Applicable major release
Name: IK8252388 (6614) Type: equipmentAlarm Package: Img.IK8252388 Raised on class: Img.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-575 IK8252391

Alarm	Attributes	Applicable major release
Name: IK8252391 (6615) Type: processingErrorAlarm Package: lmg.IK8252391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-576 IK8252401

Alarm	Attributes	Applicable major release
Name: IK8252401 (6616) Type: communicationsAlarm Package: lmg.IK8252401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-577 IK8252408

Alarm	Attributes	Applicable major release
Name: IK8252408 (6617) Type: qualityOfServiceAlarm Package: lmg.IK8252408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-578 IK8252409

Alarm	Attributes	Applicable major release
Name: IK8252409 (6618) Type: processingErrorAlarm Package: Img.IK8252409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-579 IK8252411

Alarm	Attributes	Applicable major release
Name: IK8252411 (6619) Type: equipmentAlarm Package: Img.IK8252411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-580 IK8252428

Alarm	Attributes	Applicable major release
Name: IK8252428 (6620) Type: equipmentAlarm Package: Img.IK8252428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-581 IK8252429

Alarm	Attributes	Applicable major release
Name: IK8252429 (6621) Type: equipmentAlarm Package: Img.IK8252429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		

Table 27-581 IK8252429 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-582 IK8252431

Alarm	Attributes	Applicable major release
Name: IK8252431 (6622) Type: equipmentAlarm Package: lmg.IK8252431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-583 IK8252432

Alarm	Attributes	Applicable major release
Name: IK8252432 (6623) Type: equipmentAlarm Package: lmg.IK8252432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-584 IK8252436

Alarm	Attributes	Applicable major release
Name: IK8252436 (6624) Type: equipmentAlarm Package: lmg.IK8252436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-585 IK8252437

Alarm	Attributes	Applicable major release
Name: IK8252437 (6625) Type: equipmentAlarm Package: lmg.IK8252437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-586 IK8252439

Alarm	Attributes	Applicable major release
Name: IK8252439 (6626) Type: communicationsAlarm Package: lmg.IK8252439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-587 IK8252559

Alarm	Attributes	Applicable major release
Name: IK8252559 (6627) Type: equipmentAlarm Package: lmg.IK8252559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-588 IK8252609

Alarm	Attributes	Applicable major release
Name: IK8252609 (6628) Type: processingErrorAlarm Package: lmg.IK8252609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-588 IK8252609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-589 IK8252610

Alarm	Attributes	Applicable major release
Name: IK8252610 (6629) Type: processingErrorAlarm Package: lmg.IK8252610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-590 IK8252615

Alarm	Attributes	Applicable major release
Name: IK8252615 (6630) Type: equipmentAlarm Package: lmg.IK8252615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-591 IK8252616

Alarm	Attributes	Applicable major release
Name: IK8252616 (6631) Type: environmentalAlarm Package: Img.IK8252616 Raised on class: Img.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-592 IK8252617

Alarm	Attributes	Applicable major release
Name: IK8252617 (6632) Type: environmentalAlarm Package: Img.IK8252617 Raised on class: Img.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-593 IK8252620

Alarm	Attributes	Applicable major release
Name: IK8252620 (6633) Type: equipmentAlarm Package: Img.IK8252620 Raised on class: Img.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-594 IK8252622

Alarm	Attributes	Applicable major release
Name: IK8252622 (6634) Type: environmentalAlarm Package: Img.IK8252622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-595 IK8252628

Alarm	Attributes	Applicable major release
Name: IK8252628 (6635) Type: equipmentAlarm Package: Img.IK8252628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-596 IK8252632

Alarm	Attributes	Applicable major release
Name: IK8252632 (6636) Type: processingErrorAlarm Package: Img.IK8252632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-597 IK8252633

Alarm	Attributes	Applicable major release
Name: IK8252633 (6637) Type: communicationsAlarm Package: Img.IK8252633 Raised on class: Img.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-598 IK8252636

Alarm	Attributes	Applicable major release
Name: IK8252636 (9230) Type: equipmentAlarm Package: Img.IK8252636 Raised on class: Img.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-599 IK8252648

Alarm	Attributes	Applicable major release
Name: IK8252648 (6638) Type: qualityOfServiceAlarm Package: Img.IK8252648 Raised on class: Img.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-600 IK8252657

Alarm	Attributes	Applicable major release
Name: IK8252657 (6639) Type: environmentalAlarm Package: lmg.IK8252657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-601 IK8254762

Alarm	Attributes	Applicable major release
Name: IK8254762 (6640) Type: communicationsAlarm Package: lmg.IK8254762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-602 IK8300982

Alarm	Attributes	Applicable major release
Name: IK8300982 (6641) Type: equipmentAlarm Package: lmg.IK8300982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-603 IK8300984

Alarm	Attributes	Applicable major release
Name: IK8300984 (6642) Type: processingErrorAlarm Package: Img.IK8300984 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-604 IK8300986

Alarm	Attributes	Applicable major release
Name: IK8300986 (6643) Type: equipmentAlarm Package: Img.IK8300986 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-605 IK8301008

Alarm	Attributes	Applicable major release
Name: IK8301008 (6644) Type: equipmentAlarm Package: Img.IK8301008 Raised on class: Img.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-606 IK8301010

Alarm	Attributes	Applicable major release
Name: IK8301010 (6645) Type: equipmentAlarm Package: lmg.IK8301010 Raised on class: lmg.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-607 IK8301013

Alarm	Attributes	Applicable major release
Name: IK8301013 (6646) Type: equipmentAlarm Package: lmg.IK8301013 Raised on class: lmg.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-608 IK8301018

Alarm	Attributes	Applicable major release
Name: IK8301018 (6647) Type: processingErrorAlarm Package: lmg.IK8301018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-609 IK8301023

Alarm	Attributes	Applicable major release
Name: IK8301023 (6648) Type: processingErrorAlarm Package: lmg.IK8301023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-609 IK8301023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-610 IK8301030

Alarm	Attributes	Applicable major release
Name: IK8301030 (6649) Type: equipmentAlarm Package: lmg.IK8301030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-611 IK8301033

Alarm	Attributes	Applicable major release
Name: IK8301033 (6650) Type: equipmentAlarm Package: lmg.IK8301033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-612 IK8301037

Alarm	Attributes	Applicable major release
Name: IK8301037 (6651) Type: equipmentAlarm Package: lmg.IK8301037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		

Table 27-612 IK8301037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-613 IK8301040

Alarm	Attributes	Applicable major release
Name: IK8301040 (6652) Type: environmentalAlarm Package: lmg.IK8301040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-614 IK8301060

Alarm	Attributes	Applicable major release
Name: IK8301060 (6653) Type: environmentalAlarm Package: lmg.IK8301060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-615 IK8301073

Alarm	Attributes	Applicable major release
Name: IK8301073 (6654) Type: environmentalAlarm Package: lmg.IK8301073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		

Table 27-615 IK8301073 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the Accelerator Cache Board.		

Table 27-616 IK8301091

Alarm	Attributes	Applicable major release
Name: IK8301091 (9231) Type: environmentalAlarm Package: Img.IK8301091 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-617 IK8301098

Alarm	Attributes	Applicable major release
Name: IK8301098 (6655) Type: equipmentAlarm Package: Img.IK8301098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-618 IK8301102

Alarm	Attributes	Applicable major release
Name: IK8301102 (6656) Type: environmentalAlarm Package: Img.IK8301102 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-619 IK8301105

Alarm	Attributes	Applicable major release
Name: IK8301105 (6657) Type: environmentalAlarm Package: Img.IK8301105 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-620 IK8301112

Alarm	Attributes	Applicable major release
Name: IK8301112 (6658) Type: equipmentAlarm Package: Img.IK8301112 Raised on class: Img.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-621 IK8301116

Alarm	Attributes	Applicable major release
Name: IK8301116 (6659) Type: equipmentAlarm Package: Img.IK8301116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-622 IK8301121

Alarm	Attributes	Applicable major release
Name: IK8301121 (6660) Type: environmentalAlarm Package: Img.IK8301121 Raised on class: Img.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-623 IK8301125

Alarm	Attributes	Applicable major release
Name: IK8301125 (6661) Type: environmentalAlarm Package: Img.IK8301125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-624 IK8301129

Alarm	Attributes	Applicable major release
Name: IK8301129 (6662) Type: equipmentAlarm Package: Img.IK8301129 Raised on class: Img.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-625 IK8301135

Alarm	Attributes	Applicable major release
Name: IK8301135 (6663) Type: equipmentAlarm Package: Img.IK8301135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-625 IK8301135 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-626 IK8301144

Alarm	Attributes	Applicable major release
Name: IK8301144 (6664) Type: processingErrorAlarm Package: Img.IK8301144 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-627 IK8301148

Alarm	Attributes	Applicable major release
Name: IK8301148 (6665) Type: equipmentAlarm Package: Img.IK8301148 Raised on class: Img.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-628 IK8301152

Alarm	Attributes	Applicable major release
Name: IK8301152 (6666) Type: processingErrorAlarm Package: Img.IK8301152 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		

Table 27-628 IK8301152 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-629 IK8301154

Alarm	Attributes	Applicable major release
Name: IK8301154 (6667) Type: equipmentAlarm Package: Img.IK8301154 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-630 IK8301156

Alarm	Attributes	Applicable major release
Name: IK8301156 (6668) Type: processingErrorAlarm Package: Img.IK8301156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-631 IK8301158

Alarm	Attributes	Applicable major release
Name: IK8301158 (6669) Type: processingErrorAlarm Package: Img.IK8301158 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-632 IK8301160

Alarm	Attributes	Applicable major release
Name: IK8301160 (9232) Type: communicationsAlarm Package: lmg.IK8301160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-633 IK8301163

Alarm	Attributes	Applicable major release
Name: IK8301163 (6670) Type: communicationsAlarm Package: lmg.IK8301163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-634 IK8301172

Alarm	Attributes	Applicable major release
Name: IK8301172 (6671) Type: qualityOfServiceAlarm Package: lmg.IK8301172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-635 IK8302265

Alarm	Attributes	Applicable major release
Name: IK8302265 (6672) Type: environmentalAlarm Package: Img.IK8302265 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-636 IK8302272

Alarm	Attributes	Applicable major release
Name: IK8302272 (6673) Type: environmentalAlarm Package: Img.IK8302272 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-637 IK8302279

Alarm	Attributes	Applicable major release
Name: IK8302279 (6674) Type: environmentalAlarm Package: Img.IK8302279 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-638 IK8302291

Alarm	Attributes	Applicable major release
Name: IK8302291 (6675) Type: equipmentAlarm Package: lmg.IK8302291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-639 IK8302292

Alarm	Attributes	Applicable major release
Name: IK8302292 (6676) Type: environmentalAlarm Package: lmg.IK8302292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-640 IK8302295

Alarm	Attributes	Applicable major release
Name: IK8302295 (6677) Type: equipmentAlarm Package: lmg.IK8302295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-641 IK8302302

Alarm	Attributes	Applicable major release
Name: IK8302302 (6678) Type: equipmentAlarm Package: Img.IK8302302 Raised on class: Img.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-642 IK8302337

Alarm	Attributes	Applicable major release
Name: IK8302337 (6679) Type: communicationsAlarm Package: Img.IK8302337 Raised on class: Img.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-643 IK8302341

Alarm	Attributes	Applicable major release
Name: IK8302341 (6680) Type: communicationsAlarm Package: Img.IK8302341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-644 IK8302343

Alarm	Attributes	Applicable major release
Name: IK8302343 (6681) Type: communicationsAlarm Package: lmg.IK8302343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-645 IK8302347

Alarm	Attributes	Applicable major release
Name: IK8302347 (6682) Type: communicationsAlarm Package: lmg.IK8302347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-646 IK8302349

Alarm	Attributes	Applicable major release
Name: IK8302349 (6683) Type: communicationsAlarm Package: lmg.IK8302349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-647 IK8302360

Alarm	Attributes	Applicable major release
Name: IK8302360 (6684) Type: equipmentAlarm Package: lmg.IK8302360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-648 IK8302363

Alarm	Attributes	Applicable major release
Name: IK8302363 (6685) Type: environmentalAlarm Package: lmg.IK8302363 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-649 IK8302368

Alarm	Attributes	Applicable major release
Name: IK8302368 (6686) Type: equipmentAlarm Package: lmg.IK8302368 Raised on class: lmg.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-650 IK8302369

Alarm	Attributes	Applicable major release
Name: IK8302369 (6687) Type: equipmentAlarm Package: lmg.IK8302369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-651 IK8302374

Alarm	Attributes	Applicable major release
Name: IK8302374 (6688) Type: equipmentAlarm Package: lmg.IK8302374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-652 IK8302375

Alarm	Attributes	Applicable major release
Name: IK8302375 (6689) Type: equipmentAlarm Package: lmg.IK8302375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-653 IK8302376

Alarm	Attributes	Applicable major release
Name: IK8302376 (6690) Type: equipmentAlarm Package: Img.IK8302376 Raised on class: Img.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-654 IK8302377

Alarm	Attributes	Applicable major release
Name: IK8302377 (6691) Type: equipmentAlarm Package: Img.IK8302377 Raised on class: Img.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-655 IK8302378

Alarm	Attributes	Applicable major release
Name: IK8302378 (6692) Type: equipmentAlarm Package: Img.IK8302378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-656 IK8302379

Alarm	Attributes	Applicable major release
Name: IK8302379 (6693) Type: equipmentAlarm Package: Img.IK8302379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-657 IK8302380

Alarm	Attributes	Applicable major release
Name: IK8302380 (6694) Type: equipmentAlarm Package: Img.IK8302380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-658 IK8302382

Alarm	Attributes	Applicable major release
Name: IK8302382 (6695) Type: environmentalAlarm Package: Img.IK8302382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-659 IK8302386

Alarm	Attributes	Applicable major release
Name: IK8302386 (6696) Type: equipmentAlarm Package: Img.IK8302386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-660 IK8302387

Alarm	Attributes	Applicable major release
Name: IK8302387 (6697) Type: equipmentAlarm Package: Img.IK8302387 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-661 IK8302388

Alarm	Attributes	Applicable major release
Name: IK8302388 (6698) Type: equipmentAlarm Package: Img.IK8302388 Raised on class: Img.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-662 IK8302391

Alarm	Attributes	Applicable major release
Name: IK8302391 (6699) Type: processingErrorAlarm Package: lmg.IK8302391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-663 IK8302401

Alarm	Attributes	Applicable major release
Name: IK8302401 (6700) Type: communicationsAlarm Package: lmg.IK8302401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-664 IK8302408

Alarm	Attributes	Applicable major release
Name: IK8302408 (6701) Type: qualityOfServiceAlarm Package: lmg.IK8302408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-665 IK8302409

Alarm	Attributes	Applicable major release
Name: IK8302409 (6702) Type: processingErrorAlarm Package: Img.IK8302409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-666 IK8302411

Alarm	Attributes	Applicable major release
Name: IK8302411 (6703) Type: equipmentAlarm Package: Img.IK8302411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-667 IK8302428

Alarm	Attributes	Applicable major release
Name: IK8302428 (6704) Type: equipmentAlarm Package: Img.IK8302428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-668 IK8302429

Alarm	Attributes	Applicable major release
Name: IK8302429 (6705) Type: equipmentAlarm Package: Img.IK8302429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		

Table 27-668 IK8302429 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-669 IK8302431

Alarm	Attributes	Applicable major release
Name: IK8302431 (6706) Type: equipmentAlarm Package: lmg.IK8302431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-670 IK8302432

Alarm	Attributes	Applicable major release
Name: IK8302432 (6707) Type: equipmentAlarm Package: lmg.IK8302432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-671 IK8302436

Alarm	Attributes	Applicable major release
Name: IK8302436 (6708) Type: equipmentAlarm Package: lmg.IK8302436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-672 IK8302437

Alarm	Attributes	Applicable major release
Name: IK8302437 (6709) Type: equipmentAlarm Package: lmg.IK8302437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-673 IK8302439

Alarm	Attributes	Applicable major release
Name: IK8302439 (6710) Type: communicationsAlarm Package: lmg.IK8302439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-674 IK8302559

Alarm	Attributes	Applicable major release
Name: IK8302559 (6711) Type: equipmentAlarm Package: lmg.IK8302559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-675 IK8302609

Alarm	Attributes	Applicable major release
Name: IK8302609 (6712) Type: processingErrorAlarm Package: lmg.IK8302609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-675 IK8302609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-676 IK8302610

Alarm	Attributes	Applicable major release
Name: IK8302610 (6713) Type: processingErrorAlarm Package: lmg.IK8302610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-677 IK8302615

Alarm	Attributes	Applicable major release
Name: IK8302615 (6714) Type: equipmentAlarm Package: lmg.IK8302615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-678 IK8302616

Alarm	Attributes	Applicable major release
Name: IK8302616 (6715) Type: environmentalAlarm Package: lmg.IK8302616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-679 IK8302617

Alarm	Attributes	Applicable major release
Name: IK8302617 (6716) Type: environmentalAlarm Package: lmg.IK8302617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-680 IK8302620

Alarm	Attributes	Applicable major release
Name: IK8302620 (6717) Type: equipmentAlarm Package: lmg.IK8302620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-681 IK8302622

Alarm	Attributes	Applicable major release
Name: IK8302622 (6718) Type: environmentalAlarm Package: Img.IK8302622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-682 IK8302628

Alarm	Attributes	Applicable major release
Name: IK8302628 (6719) Type: equipmentAlarm Package: Img.IK8302628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-683 IK8302632

Alarm	Attributes	Applicable major release
Name: IK8302632 (6720) Type: processingErrorAlarm Package: Img.IK8302632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-684 IK8302633

Alarm	Attributes	Applicable major release
Name: IK8302633 (6721) Type: communicationsAlarm Package: Img.IK8302633 Raised on class: Img.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-685 IK8302636

Alarm	Attributes	Applicable major release
Name: IK8302636 (9233) Type: equipmentAlarm Package: Img.IK8302636 Raised on class: Img.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-686 IK8302648

Alarm	Attributes	Applicable major release
Name: IK8302648 (6722) Type: qualityOfServiceAlarm Package: Img.IK8302648 Raised on class: Img.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-687 IK8302657

Alarm	Attributes	Applicable major release
Name: IK8302657 (6723) Type: environmentalAlarm Package: lmg.IK8302657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-688 IK8304762

Alarm	Attributes	Applicable major release
Name: IK8304762 (6724) Type: communicationsAlarm Package: lmg.IK8304762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-689 IK8350982

Alarm	Attributes	Applicable major release
Name: IK8350982 (6725) Type: equipmentAlarm Package: lmg.IK8350982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-690 IK8350984

Alarm	Attributes	Applicable major release
Name: IK8350984 (6726) Type: processingErrorAlarm Package: Img.IK8350984 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-691 IK8350986

Alarm	Attributes	Applicable major release
Name: IK8350986 (6727) Type: equipmentAlarm Package: Img.IK8350986 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-692 IK8351008

Alarm	Attributes	Applicable major release
Name: IK8351008 (6728) Type: equipmentAlarm Package: Img.IK8351008 Raised on class: Img.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-693 IK8351010

Alarm	Attributes	Applicable major release
Name: IK8351010 (6729) Type: equipmentAlarm Package: lmg.IK8351010 Raised on class: lmg.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-694 IK8351013

Alarm	Attributes	Applicable major release
Name: IK8351013 (6730) Type: equipmentAlarm Package: lmg.IK8351013 Raised on class: lmg.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-695 IK8351018

Alarm	Attributes	Applicable major release
Name: IK8351018 (6731) Type: processingErrorAlarm Package: lmg.IK8351018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-696 IK8351023

Alarm	Attributes	Applicable major release
Name: IK8351023 (6732) Type: processingErrorAlarm Package: lmg.IK8351023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-696 IK8351023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-697 IK8351030

Alarm	Attributes	Applicable major release
Name: IK8351030 (6733) Type: equipmentAlarm Package: lmg.IK8351030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-698 IK8351033

Alarm	Attributes	Applicable major release
Name: IK8351033 (6734) Type: equipmentAlarm Package: lmg.IK8351033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-699 IK8351037

Alarm	Attributes	Applicable major release
Name: IK8351037 (6735) Type: equipmentAlarm Package: lmg.IK8351037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		

Table 27-699 IK8351037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-700 IK8351040

Alarm	Attributes	Applicable major release
Name: IK8351040 (6736) Type: environmentalAlarm Package: lmg.IK8351040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-701 IK8351060

Alarm	Attributes	Applicable major release
Name: IK8351060 (6737) Type: environmentalAlarm Package: lmg.IK8351060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-702 IK8351073

Alarm	Attributes	Applicable major release
Name: IK8351073 (6738) Type: environmentalAlarm Package: lmg.IK8351073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		

Table 27-702 IK8351073 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the Accelerator Cache Board.		

Table 27-703 IK8351091

Alarm	Attributes	Applicable major release
Name: IK8351091 (9234) Type: environmentalAlarm Package: Img.IK8351091 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-704 IK8351098

Alarm	Attributes	Applicable major release
Name: IK8351098 (6739) Type: equipmentAlarm Package: Img.IK8351098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-705 IK8351102

Alarm	Attributes	Applicable major release
Name: IK8351102 (6740) Type: environmentalAlarm Package: Img.IK8351102 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-706 IK8351105

Alarm	Attributes	Applicable major release
Name: IK8351105 (6741) Type: environmentalAlarm Package: lmg.IK8351105 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-707 IK8351112

Alarm	Attributes	Applicable major release
Name: IK8351112 (6742) Type: equipmentAlarm Package: lmg.IK8351112 Raised on class: lmg.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-708 IK8351116

Alarm	Attributes	Applicable major release
Name: IK8351116 (6743) Type: equipmentAlarm Package: lmg.IK8351116 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-709 IK8351121

Alarm	Attributes	Applicable major release
Name: IK8351121 (6744) Type: environmentalAlarm Package: Img.IK8351121 Raised on class: Img.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-710 IK8351125

Alarm	Attributes	Applicable major release
Name: IK8351125 (6745) Type: environmentalAlarm Package: Img.IK8351125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-711 IK8351129

Alarm	Attributes	Applicable major release
Name: IK8351129 (6746) Type: equipmentAlarm Package: Img.IK8351129 Raised on class: Img.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-712 IK8351135

Alarm	Attributes	Applicable major release
Name: IK8351135 (6747) Type: equipmentAlarm Package: Img.IK8351135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-712 IK8351135 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-713 IK8351144

Alarm	Attributes	Applicable major release
Name: IK8351144 (6748) Type: processingErrorAlarm Package: lmg.IK8351144 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-714 IK8351148

Alarm	Attributes	Applicable major release
Name: IK8351148 (6749) Type: equipmentAlarm Package: lmg.IK8351148 Raised on class: lmg.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-715 IK8351152

Alarm	Attributes	Applicable major release
Name: IK8351152 (6750) Type: processingErrorAlarm Package: lmg.IK8351152 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		

Table 27-715 IK8351152 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-716 IK8351154

Alarm	Attributes	Applicable major release
Name: IK8351154 (6751) Type: equipmentAlarm Package: lmg.IK8351154 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-717 IK8351156

Alarm	Attributes	Applicable major release
Name: IK8351156 (6752) Type: processingErrorAlarm Package: lmg.IK8351156 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-718 IK8351158

Alarm	Attributes	Applicable major release
Name: IK8351158 (6753) Type: processingErrorAlarm Package: lmg.IK8351158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-719 IK8351160

Alarm	Attributes	Applicable major release
Name: IK8351160 (9235) Type: communicationsAlarm Package: lmg.IK8351160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-720 IK8351163

Alarm	Attributes	Applicable major release
Name: IK8351163 (6754) Type: communicationsAlarm Package: lmg.IK8351163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-721 IK8351172

Alarm	Attributes	Applicable major release
Name: IK8351172 (6755) Type: qualityOfServiceAlarm Package: lmg.IK8351172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-722 IK8352265

Alarm	Attributes	Applicable major release
Name: IK8352265 (6756) Type: environmentalAlarm Package: lmg.IK8352265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-723 IK8352272

Alarm	Attributes	Applicable major release
Name: IK8352272 (6757) Type: environmentalAlarm Package: lmg.IK8352272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-724 IK8352279

Alarm	Attributes	Applicable major release
Name: IK8352279 (6758) Type: environmentalAlarm Package: lmg.IK8352279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-725 IK8352291

Alarm	Attributes	Applicable major release
Name: IK8352291 (6759) Type: equipmentAlarm Package: lmg.IK8352291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-726 IK8352292

Alarm	Attributes	Applicable major release
Name: IK8352292 (6760) Type: environmentalAlarm Package: lmg.IK8352292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-727 IK8352295

Alarm	Attributes	Applicable major release
Name: IK8352295 (6761) Type: equipmentAlarm Package: lmg.IK8352295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-728 IK8352302

Alarm	Attributes	Applicable major release
Name: IK8352302 (6762) Type: equipmentAlarm Package: Img.IK8352302 Raised on class: Img.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-729 IK8352337

Alarm	Attributes	Applicable major release
Name: IK8352337 (6763) Type: communicationsAlarm Package: Img.IK8352337 Raised on class: Img.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-730 IK8352341

Alarm	Attributes	Applicable major release
Name: IK8352341 (6764) Type: communicationsAlarm Package: Img.IK8352341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-731 IK8352343

Alarm	Attributes	Applicable major release
Name: IK8352343 (6765) Type: communicationsAlarm Package: lmg.IK8352343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-732 IK8352347

Alarm	Attributes	Applicable major release
Name: IK8352347 (6766) Type: communicationsAlarm Package: lmg.IK8352347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-733 IK8352349

Alarm	Attributes	Applicable major release
Name: IK8352349 (6767) Type: communicationsAlarm Package: lmg.IK8352349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-734 IK8352360

Alarm	Attributes	Applicable major release
Name: IK8352360 (6768) Type: equipmentAlarm Package: lmg.IK8352360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-735 IK8352363

Alarm	Attributes	Applicable major release
Name: IK8352363 (6769) Type: environmentalAlarm Package: lmg.IK8352363 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-736 IK8352368

Alarm	Attributes	Applicable major release
Name: IK8352368 (6770) Type: equipmentAlarm Package: lmg.IK8352368 Raised on class: lmg.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-737 IK8352369

Alarm	Attributes	Applicable major release
Name: IK8352369 (6771) Type: equipmentAlarm Package: lmg.IK8352369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-738 IK8352374

Alarm	Attributes	Applicable major release
Name: IK8352374 (6772) Type: equipmentAlarm Package: lmg.IK8352374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-739 IK8352375

Alarm	Attributes	Applicable major release
Name: IK8352375 (6773) Type: equipmentAlarm Package: lmg.IK8352375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-740 IK8352376

Alarm	Attributes	Applicable major release
Name: IK8352376 (6774) Type: equipmentAlarm Package: Img.IK8352376 Raised on class: Img.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-741 IK8352377

Alarm	Attributes	Applicable major release
Name: IK8352377 (6775) Type: equipmentAlarm Package: Img.IK8352377 Raised on class: Img.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-742 IK8352378

Alarm	Attributes	Applicable major release
Name: IK8352378 (6776) Type: equipmentAlarm Package: Img.IK8352378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-743 IK8352379

Alarm	Attributes	Applicable major release
Name: IK8352379 (6777) Type: equipmentAlarm Package: lmg.IK8352379 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-744 IK8352380

Alarm	Attributes	Applicable major release
Name: IK8352380 (6778) Type: equipmentAlarm Package: lmg.IK8352380 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-745 IK8352382

Alarm	Attributes	Applicable major release
Name: IK8352382 (6779) Type: environmentalAlarm Package: lmg.IK8352382 Raised on class: lmg.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-746 IK8352386

Alarm	Attributes	Applicable major release
Name: IK8352386 (6780) Type: equipmentAlarm Package: Img.IK8352386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-747 IK8352387

Alarm	Attributes	Applicable major release
Name: IK8352387 (6781) Type: equipmentAlarm Package: Img.IK8352387 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-748 IK8352388

Alarm	Attributes	Applicable major release
Name: IK8352388 (6782) Type: equipmentAlarm Package: Img.IK8352388 Raised on class: Img.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-749 IK8352391

Alarm	Attributes	Applicable major release
Name: IK8352391 (6783) Type: processingErrorAlarm Package: lmg.IK8352391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-750 IK8352401

Alarm	Attributes	Applicable major release
Name: IK8352401 (6784) Type: communicationsAlarm Package: lmg.IK8352401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-751 IK8352408

Alarm	Attributes	Applicable major release
Name: IK8352408 (6785) Type: qualityOfServiceAlarm Package: lmg.IK8352408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-752 IK8352409

Alarm	Attributes	Applicable major release
Name: IK8352409 (6786) Type: processingErrorAlarm Package: Img.IK8352409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-753 IK8352411

Alarm	Attributes	Applicable major release
Name: IK8352411 (6787) Type: equipmentAlarm Package: Img.IK8352411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-754 IK8352428

Alarm	Attributes	Applicable major release
Name: IK8352428 (6788) Type: equipmentAlarm Package: Img.IK8352428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-755 IK8352429

Alarm	Attributes	Applicable major release
Name: IK8352429 (6789) Type: equipmentAlarm Package: Img.IK8352429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		

Table 27-755 IK8352429 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-756 IK8352431

Alarm	Attributes	Applicable major release
Name: IK8352431 (6790) Type: equipmentAlarm Package: lmg.IK8352431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-757 IK8352432

Alarm	Attributes	Applicable major release
Name: IK8352432 (6791) Type: equipmentAlarm Package: lmg.IK8352432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-758 IK8352436

Alarm	Attributes	Applicable major release
Name: IK8352436 (6792) Type: equipmentAlarm Package: lmg.IK8352436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-759 IK8352437

Alarm	Attributes	Applicable major release
Name: IK8352437 (6793) Type: equipmentAlarm Package: lmg.IK8352437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-760 IK8352439

Alarm	Attributes	Applicable major release
Name: IK8352439 (6794) Type: communicationsAlarm Package: lmg.IK8352439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-761 IK8352559

Alarm	Attributes	Applicable major release
Name: IK8352559 (6795) Type: equipmentAlarm Package: lmg.IK8352559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-762 IK8352609

Alarm	Attributes	Applicable major release
Name: IK8352609 (6796) Type: processingErrorAlarm Package: lmg.IK8352609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-762 IK8352609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-763 IK8352610

Alarm	Attributes	Applicable major release
Name: IK8352610 (6797) Type: processingErrorAlarm Package: lmg.IK8352610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-764 IK8352615

Alarm	Attributes	Applicable major release
Name: IK8352615 (6798) Type: equipmentAlarm Package: lmg.IK8352615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-765 IK8352616

Alarm	Attributes	Applicable major release
Name: IK8352616 (6799) Type: environmentalAlarm Package: lmg.IK8352616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-766 IK8352617

Alarm	Attributes	Applicable major release
Name: IK8352617 (6800) Type: environmentalAlarm Package: lmg.IK8352617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-767 IK8352620

Alarm	Attributes	Applicable major release
Name: IK8352620 (6801) Type: equipmentAlarm Package: lmg.IK8352620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-768 IK8352622

Alarm	Attributes	Applicable major release
Name: IK8352622 (6802) Type: environmentalAlarm Package: Img.IK8352622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-769 IK8352628

Alarm	Attributes	Applicable major release
Name: IK8352628 (6803) Type: equipmentAlarm Package: Img.IK8352628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-770 IK8352632

Alarm	Attributes	Applicable major release
Name: IK8352632 (6804) Type: processingErrorAlarm Package: Img.IK8352632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-771 IK8352633

Alarm	Attributes	Applicable major release
Name: IK8352633 (6805) Type: communicationsAlarm Package: Img.IK8352633 Raised on class: Img.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-772 IK8352636

Alarm	Attributes	Applicable major release
Name: IK8352636 (9236) Type: equipmentAlarm Package: Img.IK8352636 Raised on class: Img.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-773 IK8352648

Alarm	Attributes	Applicable major release
Name: IK8352648 (6806) Type: qualityOfServiceAlarm Package: Img.IK8352648 Raised on class: Img.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-774 IK8352657

Alarm	Attributes	Applicable major release
Name: IK8352657 (6807) Type: environmentalAlarm Package: lmg.IK8352657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-775 IK8354762

Alarm	Attributes	Applicable major release
Name: IK8354762 (6808) Type: communicationsAlarm Package: lmg.IK8354762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-776 IK8360000

Alarm	Attributes	Applicable major release
Name: IK8360000 (9790) Type: processingErrorAlarm Package: lmg.IK8360000 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical service or resource not available during initialization Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: The server is not able to provide service due to a process or interface failure, or a missing file. Alarm is cleared by the system on server restart.\nReason: Critical service or resource not available during initialization		
Remedial action: Check the LMG log files to determine the root cause		

Table 27-777 IK8360001

Alarm	Attributes	Applicable major release
Name: IK8360001 (9791) Type: processingErrorAlarm Package: lmg.IK8360001 Raised on class: lmg.FRU	Severity: critical Specific problem: Server health check audit detected critical service or resource not available Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: The server is not able to provide service due to a process or interface failure, or a missing file. Alarm is cleared by the system on server restart or if the server health check audit runs successfully, or when the service is restarted.\nReason: Server health check audit detected critical service or resource not available		
Remedial action: Check the LMG log files to determine the root cause		

Table 27-778 IK8360005

Alarm	Attributes	Applicable major release
Name: IK8360005 (9795) Type: processingErrorAlarm Package: lmg.IK8360005 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: mcdp alarm trap v1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: mcdp alarm alarm v1.\nAlarm is cleared by the system.\nReason: alarmTrapV1		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-779 IK8360006

Alarm	Attributes	Applicable major release
Name: IK8360006 (9796) Type: processingErrorAlarm Package: lmg.IK8360006 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Trap associated to an alarm of the managed element Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: Trap associated to an alarm of the managed element.\nAlarm is cleared by the system when the device is restarted.\nReason: alarmTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-780 IK8360007

Alarm	Attributes	Applicable major release
Name: IK8360007 (9797) Type: processingErrorAlarm Package: lmg.IK8360007 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: softwareFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.MG
Description: Trap associated to an alarm while executing software operation (download, activation, validation, reject, backup).\nAlarm is cleared by the system.\nReason: softwareFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-781 IK8361018

Alarm	Attributes	Applicable major release
Name: IK8361018 (10324) Type: processingErrorAlarm Package: lmg.IK8361018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-782 IK8361033

Alarm	Attributes	Applicable major release
Name: IK8361033 (10325) Type: equipmentAlarm Package: lmg.IK8361033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-783 IK8361040

Alarm	Attributes	Applicable major release
Name: IK8361040 (10326) Type: environmentalAlarm Package: lmg.IK8361040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG

Table 27-783 IK8361040 (continued)

Alarm	Attributes	Applicable major release
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-784 IK8361091

Alarm	Attributes	Applicable major release
Name: IK8361091 (10327) Type: environmentalAlarm Package: lmg.IK8361091 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-785 IK8361102

Alarm	Attributes	Applicable major release
Name: IK8361102 (10328) Type: environmentalAlarm Package: lmg.IK8361102 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-786 IK8361105

Alarm	Attributes	Applicable major release
Name: IK8361105 (10329) Type: environmentalAlarm Package: lmg.IK8361105 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-787 IK8361125

Alarm	Attributes	Applicable major release
Name: IK8361125 (10330) Type: environmentalAlarm Package: lmg.IK8361125 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-788 IK8361135

Alarm	Attributes	Applicable major release
Name: IK8361135 (10331) Type: equipmentAlarm Package: lmg.IK8361135 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-789 IK8361154

Alarm	Attributes	Applicable major release
Name: IK8361154 (10332) Type: equipmentAlarm Package: lmg.IK8361154 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-790 IK8361160

Alarm	Attributes	Applicable major release
Name: IK8361160 (10333) Type: communicationsAlarm Package: lmg.IK8361160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG

Table 27-790 IK8361160 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-791 IK8361163

Alarm	Attributes	Applicable major release
Name: IK8361163 (10334) Type: communicationsAlarm Package: lmg.IK8361163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-792 IK8362337

Alarm	Attributes	Applicable major release
Name: IK8362337 (10335) Type: communicationsAlarm Package: lmg.IK8362337 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-793 IK8362341

Alarm	Attributes	Applicable major release
Name: IK8362341 (10336) Type: communicationsAlarm Package: lmg.IK8362341 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG

Table 27-793 IK8362341 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-794 IK8362343

Alarm	Attributes	Applicable major release
Name: IK8362343 (10337) Type: communicationsAlarm Package: lmg.IK8362343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-795 IK8362349

Alarm	Attributes	Applicable major release
Name: IK8362349 (10338) Type: communicationsAlarm Package: lmg.IK8362349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-796 IK8362360

Alarm	Attributes	Applicable major release
Name: IK8362360 (10339) Type: equipmentAlarm Package: lmg.IK8362360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-797 IK8362401

Alarm	Attributes	Applicable major release
Name: IK8362401 (10340) Type: communicationsAlarm Package: lmg.IK8362401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-798 IK8362409

Alarm	Attributes	Applicable major release
Name: IK8362409 (10341) Type: processingErrorAlarm Package: lmg.IK8362409 Raised on class: lmg.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-799 IK8362462

Alarm	Attributes	Applicable major release
Name: IK8362462 (10342) Type: environmentalAlarm Package: lmg.IK8362462 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR16.1.MG
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-800 IK8362464

Alarm	Attributes	Applicable major release
Name: IK8362464 (10343) Type: equipmentAlarm Package: lmg.IK8362464 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-801 IK8362468

Alarm	Attributes	Applicable major release
Name: IK8362468 (10344) Type: equipmentAlarm Package: lmg.IK8362468 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-802 IK8362494

Alarm	Attributes	Applicable major release
Name: IK8362494 (10345) Type: equipmentAlarm Package: lmg.IK8362494 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutpu-tOverload		

Table 27-802 IK8362494 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-803 IK8362496

Alarm	Attributes	Applicable major release
Name: IK8362496 (10346) Type: environmentalAlarm Package: lmg.IK8362496 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-804 IK8362508

Alarm	Attributes	Applicable major release
Name: IK8362508 (10347) Type: equipmentAlarm Package: lmg.IK8362508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-805 IK8362510

Alarm	Attributes	Applicable major release
Name: IK8362510 (10348) Type: environmentalAlarm Package: lmg.IK8362510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-806 IK8362518

Alarm	Attributes	Applicable major release
Name: IK8362518 (10349) Type: equipmentAlarm Package: lmg.IK8362518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-807 IK8362531

Alarm	Attributes	Applicable major release
Name: IK8362531 (10350) Type: equipmentAlarm Package: lmg.IK8362531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-808 IK8362533

Alarm	Attributes	Applicable major release
Name: IK8362533 (10351) Type: equipmentAlarm Package: lmg.IK8362533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInputOutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-809 IK8362534

Alarm	Attributes	Applicable major release
Name: IK8362534 (10352) Type: environmentalAlarm Package: lmg.IK8362534 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTemperatureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-810 IK8362536

Alarm	Attributes	Applicable major release
Name: IK8362536 (10353) Type: equipmentAlarm Package: lmg.IK8362536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassOnAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-811 IK8362539

Alarm	Attributes	Applicable major release
Name: IK8362539 (10354) Type: equipmentAlarm Package: lmg.IK8362539 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-812 IK8362541

Alarm	Attributes	Applicable major release
Name: IK8362541 (10355) Type: environmentalAlarm Package: lmg.IK8362541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-813 IK8362543

Alarm	Attributes	Applicable major release
Name: IK8362543 (10356) Type: equipmentAlarm Package: lmg.IK8362543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If the problem persists, contact NOKIA customer support.		

Table 27-814 IK8362546

Alarm	Attributes	Applicable major release
Name: IK8362546 (10357) Type: equipmentAlarm Package: lmg.IK8362546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-815 IK8362548

Alarm	Attributes	Applicable major release
Name: IK8362548 (10358) Type: environmentalAlarm Package: lmg.IK8362548 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If the problem persists, contact NOKIA customer support.		

Table 27-816 IK8362550

Alarm	Attributes	Applicable major release
Name: IK8362550 (10359) Type: environmentalAlarm Package: lmg.IK8362550 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If the problem persists, contact NOKIA customer support.		

Table 27-817 IK8362552

Alarm	Attributes	Applicable major release
Name: IK8362552 (10360) Type: processingErrorAlarm Package: lmg.IK8362552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-818 IK8362554

Alarm	Attributes	Applicable major release
Name: IK8362554 (10361) Type: equipmentAlarm Package: lmg.IK8362554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-819 IK8362556

Alarm	Attributes	Applicable major release
Name: IK8362556 (10362) Type: equipmentAlarm Package: lmg.IK8362556 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-820 IK8362559

Alarm	Attributes	Applicable major release
Name: IK8362559 (10363) Type: equipmentAlarm Package: lmg.IK8362559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-821 IK8362609

Alarm	Attributes	Applicable major release
Name: IK8362609 (10364) Type: processingErrorAlarm Package: lmg.IK8362609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-821 IK8362609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-822 IK8362633

Alarm	Attributes	Applicable major release
Name: IK8362633 (10365) Type: communicationsAlarm Package: lmg.IK8362633 Raised on class: lmg.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-823 IK8362636

Alarm	Attributes	Applicable major release
Name: IK8362636 (10366) Type: equipmentAlarm Package: lmg.IK8362636 Raised on class: lmg.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-824 IK8362648

Alarm	Attributes	Applicable major release
Name: IK8362648 (10367) Type: qualityOfServiceAlarm Package: lmg.IK8362648 Raised on class: lmg.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG

Table 27-824 IK8362648 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-825 IK8362657

Alarm	Attributes	Applicable major release
Name: IK8362657 (10368) Type: environmentalAlarm Package: lmg.IK8362657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-826 IK8362748

Alarm	Attributes	Applicable major release
Name: IK8362748 (10369) Type: equipmentAlarm Package: lmg.IK8362748 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: fluteModuleAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Alarm notification\nAlarm is cleared by the system.\nReason: fluteModuleAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-827 IK8367481

Alarm	Attributes	Applicable major release
Name: IK8367481 (10370) Type: equipmentAlarm Package: lmg.IK8367481 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.		
Remedial action: No action is required.		

Table 27-828 IK8367482

Alarm	Attributes	Applicable major release
Name: IK8367482 (10371) Type: equipmentAlarm Package: Img.IK8367482 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.		
Remedial action: No action is required.		

Table 27-829 IK8367483

Alarm	Attributes	Applicable major release
Name: IK8367483 (10372) Type: equipmentAlarm Package: Img.IK8367483 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.		
Remedial action: No action is required.		

Table 27-830 IK8367484

Alarm	Attributes	Applicable major release
Name: IK8367484 (10373) Type: equipmentAlarm Package: Img.IK8367484 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.		
Remedial action: No action is required.		

Table 27-831 IK8367485

Alarm	Attributes	Applicable major release
Name: IK8367485 (10374) Type: equipmentAlarm Package: Img.IK8367485 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.		
Remedial action: No action is required.		

Table 27-832 IK8367486

Alarm	Attributes	Applicable major release
Name: IK8367486 (10375) Type: equipmentAlarm Package: lmg.IK8367486 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-833 IK8367487

Alarm	Attributes	Applicable major release
Name: IK8367487 (10376) Type: equipmentAlarm Package: lmg.IK8367487 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-834 IK8367488

Alarm	Attributes	Applicable major release
Name: IK8367488 (10377) Type: equipmentAlarm Package: lmg.IK8367488 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-835 IK8367489

Alarm	Attributes	Applicable major release
Name: IK8367489 (10378) Type: equipmentAlarm Package: lmg.IK8367489 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.		

Table 27-835 IK8367489 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-836 IK8367490

Alarm	Attributes	Applicable major release
Name: IK8367490 (10379) Type: equipmentAlarm Package: Img.IK8367490 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-837 IK8367491

Alarm	Attributes	Applicable major release
Name: IK8367491 (10380) Type: equipmentAlarm Package: Img.IK8367491 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-838 IK8367500

Alarm	Attributes	Applicable major release
Name: IK8367500 (10381) Type: equipmentAlarm Package: Img.IK8367500 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes degraded.		
Remedial action: No action is required.		

Table 27-839 IK8367501

Alarm	Attributes	Applicable major release
Name: IK8367501 (10382) Type: equipmentAlarm Package: lmg.IK8367501 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes failed.		
Remedial action: No action is required.		

Table 27-840 IK8367502

Alarm	Attributes	Applicable major release
Name: IK8367502 (10383) Type: equipmentAlarm Package: lmg.IK8367502 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes degraded.		
Remedial action: No action is required.		

Table 27-841 IK8367503

Alarm	Attributes	Applicable major release
Name: IK8367503 (10384) Type: equipmentAlarm Package: lmg.IK8367503 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes failed.		
Remedial action: No action is required.		

Table 27-842 IK8367504

Alarm	Attributes	Applicable major release
Name: IK8367504 (10385) Type: equipmentAlarm Package: lmg.IK8367504 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes degraded.		

Table 27-842 IK8367504 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-843 IK8367505

Alarm	Attributes	Applicable major release
Name: IK8367505 (10386) Type: equipmentAlarm Package: lmg.IK8367505 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes failed.		
Remedial action: No action is required.		

Table 27-844 IK8367508

Alarm	Attributes	Applicable major release
Name: IK8367508 (10387) Type: equipmentAlarm Package: lmg.IK8367508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-845 IK8367509

Alarm	Attributes	Applicable major release
Name: IK8367509 (10388) Type: equipmentAlarm Package: lmg.IK8367509 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-846 IK8367510

Alarm	Attributes	Applicable major release
Name: IK8367510 (10389) Type: equipmentAlarm Package: lmg.IK8367510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: External Array Redundant Controller Active. This event signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.		
Remedial action: No action is required.		

Table 27-847 IK8367511

Alarm	Attributes	Applicable major release
Name: IK8367511 (10390) Type: equipmentAlarm Package: lmg.IK8367511 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-848 IK8367512

Alarm	Attributes	Applicable major release
Name: IK8367512 (10391) Type: equipmentAlarm Package: lmg.IK8367512 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-849 IK8367513

Alarm	Attributes	Applicable major release
Name: IK8367513 (10392) Type: equipmentAlarm Package: Img.IK8367513 Raised on class: Img.FRU	Severity: indeterminate Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log		
Remedial action: No action is required.		

Table 27-850 IK8367514

Alarm	Attributes	Applicable major release
Name: IK8367514 (10393) Type: equipmentAlarm Package: Img.IK8367514 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.		
Remedial action: No action is required.		

Table 27-851 IK8367515

Alarm	Attributes	Applicable major release
Name: IK8367515 (10394) Type: equipmentAlarm Package: Img.IK8367515 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-852 IK8367516

Alarm	Attributes	Applicable major release
Name: IK8367516 (10395) Type: equipmentAlarm Package: Img.IK8367516 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-853 IK8367517

Alarm	Attributes	Applicable major release
Name: IK8367517 (10396) Type: equipmentAlarm Package: lmg.IK8367517 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-854 IK8367518

Alarm	Attributes	Applicable major release
Name: IK8367518 (10397) Type: equipmentAlarm Package: lmg.IK8367518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-855 IK8367519

Alarm	Attributes	Applicable major release
Name: IK8367519 (10398) Type: equipmentAlarm Package: lmg.IK8367519 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.		
Remedial action: No action is required.		

Table 27-856 IK8367520

Alarm	Attributes	Applicable major release
Name: IK8367520 (10399) Type: equipmentAlarm Package: lmg.IK8367520 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.		

Table 27-856 IK8367520 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-857 IK8367521

Alarm	Attributes	Applicable major release
Name: IK8367521 (10400) Type: equipmentAlarm Package: Img.IK8367521 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.		
Remedial action: No action is required.		

Table 27-858 IK8367522

Alarm	Attributes	Applicable major release
Name: IK8367522 (10401) Type: equipmentAlarm Package: Img.IK8367522 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.		
Remedial action: No action is required.		

Table 27-859 IK8367523

Alarm	Attributes	Applicable major release
Name: IK8367523 (10402) Type: equipmentAlarm Package: Img.IK8367523 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.		
Remedial action: No action is required.		

Table 27-860 IK8367524

Alarm	Attributes	Applicable major release
Name: IK8367524 (10403) Type: equipmentAlarm Package: lmg.IK8367524 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.		
Remedial action: No action is required.		

Table 27-861 IK8367525

Alarm	Attributes	Applicable major release
Name: IK8367525 (10404) Type: equipmentAlarm Package: lmg.IK8367525 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.		
Remedial action: No action is required.		

Table 27-862 IK8367526

Alarm	Attributes	Applicable major release
Name: IK8367526 (10405) Type: equipmentAlarm Package: lmg.IK8367526 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.		
Remedial action: No action is required.		

Table 27-863 IK8367527

Alarm	Attributes	Applicable major release
Name: IK8367527 (10406) Type: equipmentAlarm Package: Img.IK8367527 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.		
Remedial action: No action is required.		

Table 27-864 IK8367528

Alarm	Attributes	Applicable major release
Name: IK8367528 (10407) Type: equipmentAlarm Package: Img.IK8367528 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-865 IK8367529

Alarm	Attributes	Applicable major release
Name: IK8367529 (10408) Type: equipmentAlarm Package: Img.IK8367529 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-866 IK8367530

Alarm	Attributes	Applicable major release
Name: IK8367530 (10409) Type: equipmentAlarm Package: lmg.IK8367530 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.		
Remedial action: No action is required.		

Table 27-867 IK8367531

Alarm	Attributes	Applicable major release
Name: IK8367531 (10410) Type: equipmentAlarm Package: lmg.IK8367531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the configured redundant NIC becomes the active NIC.		
Remedial action: No action is required.		

Table 27-868 IK8367532

Alarm	Attributes	Applicable major release
Name: IK8367532 (10411) Type: equipmentAlarm Package: lmg.IK8367532 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.MG
Description: This event is a send to the user to notify him of a Critical Software Update.		
Remedial action: No action is required.		

Table 27-869 IK8367533

Alarm	Attributes	Applicable major release
Name: IK8367533 (10412) Type: equipmentAlarm Package: lmg.IK8367533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-869 IK8367533 (continued)

Alarm	Attributes	Applicable major release
Description: Controller Active. This event signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.		
Remedial action: No action is required.		

Table 27-870 IK8367534

Alarm	Attributes	Applicable major release
Name: IK8367534 (10413) Type: equipmentAlarm Package: lmg.IK8367534 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-871 IK8367535

Alarm	Attributes	Applicable major release
Name: IK8367535 (10414) Type: equipmentAlarm Package: lmg.IK8367535 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Accelerator Board Bad Data. This event signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-872 IK8367536

Alarm	Attributes	Applicable major release
Name: IK8367536 (10415) Type: equipmentAlarm Package: lmg.IK8367536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the array accelerator cache board.		
Remedial action: No action is required.		

Table 27-873 IK8367537

Alarm	Attributes	Applicable major release
Name: IK8367537 (10416) Type: equipmentAlarm Package: Img.IK8367537 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-874 IK8367538

Alarm	Attributes	Applicable major release
Name: IK8367538 (10417) Type: equipmentAlarm Package: Img.IK8367538 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-875 IK8367539

Alarm	Attributes	Applicable major release
Name: IK8367539 (10418) Type: equipmentAlarm Package: Img.IK8367539 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Cache Module Board Bad Data. This event signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-876 IK8367540

Alarm	Attributes	Applicable major release
Name: IK8367540 (10419) Type: equipmentAlarm Package: Img.IK8367540 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG

Table 27-876 IK8367540 (continued)

Alarm	Attributes	Applicable major release
Description: Cache Module Board Backup Power Source Failed. This event signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-877 IK8367541

Alarm	Attributes	Applicable major release
Name: IK8367541 (10420) Type: equipmentAlarm Package: lmg.IK8367541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-878 IK8367542

Alarm	Attributes	Applicable major release
Name: IK8367542 (10421) Type: equipmentAlarm Package: lmg.IK8367542 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-879 IK8367543

Alarm	Attributes	Applicable major release
Name: IK8367543 (10422) Type: equipmentAlarm Package: lmg.IK8367543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.		
Remedial action: No action is required.		

Table 27-880 IK8367545

Alarm	Attributes	Applicable major release
Name: IK8367545 (10423) Type: equipmentAlarm Package: lmg.IK8367545 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.		
Remedial action: No action is required.		

Table 27-881 IK8367546

Alarm	Attributes	Applicable major release
Name: IK8367546 (10424) Type: equipmentAlarm Package: lmg.IK8367546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to failed. This event signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-882 IK8367547

Alarm	Attributes	Applicable major release
Name: IK8367547 (10425) Type: equipmentAlarm Package: lmg.IK8367547 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to degraded. This event signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-883 IK8367548

Alarm	Attributes	Applicable major release
Name: IK8367548 (10426) Type: equipmentAlarm Package: Img.IK8367548 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to failed. This event signifies that a power supply has failed.		
Remedial action: No action is required.		

Table 27-884 IK8367549

Alarm	Attributes	Applicable major release
Name: IK8367549 (10427) Type: equipmentAlarm Package: Img.IK8367549 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to degraded. This event signifies that a power supply has degraded.		
Remedial action: No action is required.		

Table 27-885 IK8367550

Alarm	Attributes	Applicable major release
Name: IK8367550 (10428) Type: equipmentAlarm Package: Img.IK8367550 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem is no longer in a redundant state.		
Remedial action: No action is required.		

Table 27-886 IK8367551

Alarm	Attributes	Applicable major release
Name: IK8367551 (10429) Type: equipmentAlarm Package: Img.IK8367551 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power supply detected an input line voltage problem.		

Table 27-886 IK8367551 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-887 IK8367552

Alarm	Attributes	Applicable major release
Name: IK8367552 (10430) Type: equipmentAlarm Package: lmg.IK8367552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem overload condition.		
Remedial action: No action is required.		

Table 27-888 IK8367553

Alarm	Attributes	Applicable major release
Name: IK8367553 (10431) Type: equipmentAlarm Package: lmg.IK8367553 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.		
Remedial action: No action is required.		

Table 27-889 IK8367554

Alarm	Attributes	Applicable major release
Name: IK8367554 (10432) Type: equipmentAlarm Package: lmg.IK8367554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.		
Remedial action: No action is required.		

Table 27-890 IK8367555

Alarm	Attributes	Applicable major release
Name: IK8367555 (10433) Type: equipmentAlarm Package: Img.IK8367555 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.		
Remedial action: No action is required.		

Table 27-891 IK8367556

Alarm	Attributes	Applicable major release
Name: IK8367556 (10434) Type: equipmentAlarm Package: Img.IK8367556 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-892 IK8367557

Alarm	Attributes	Applicable major release
Name: IK8367557 (10435) Type: equipmentAlarm Package: Img.IK8367557 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-893 IK8367558

Alarm	Attributes	Applicable major release
Name: IK8367558 (10436) Type: equipmentAlarm Package: Img.IK8367558 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Fuse open. The fuse has been tripped.		

Table 27-893 IK8367558 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-894 IK8367559

Alarm	Attributes	Applicable major release
Name: IK8367559 (10437) Type: equipmentAlarm Package: lmg.IK8367559 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.		
Remedial action: No action is required.		

Table 27-895 IK8367560

Alarm	Attributes	Applicable major release
Name: IK8367560 (10438) Type: equipmentAlarm Package: lmg.IK8367560 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.		
Remedial action: No action is required.		

Table 27-896 IK8367561

Alarm	Attributes	Applicable major release
Name: IK8367561 (10439) Type: equipmentAlarm Package: lmg.IK8367561 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.		
Remedial action: No action is required.		

Table 27-897 IK8367562

Alarm	Attributes	Applicable major release
Name: IK8367562 (10440) Type: equipmentAlarm Package: Img.IK8367562 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.		
Remedial action: No action is required.		

Table 27-898 IK8367563

Alarm	Attributes	Applicable major release
Name: IK8367563 (10441) Type: equipmentAlarm Package: Img.IK8367563 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.		
Remedial action: No action is required.		

Table 27-899 IK8367564

Alarm	Attributes	Applicable major release
Name: IK8367564 (10442) Type: equipmentAlarm Package: Img.IK8367564 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.		
Remedial action: No action is required.		

Table 27-900 IK8367565

Alarm	Attributes	Applicable major release
Name: IK8367565 (10443) Type: equipmentAlarm Package: Img.IK8367565 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG

Table 27-900 IK8367565 (continued)

Alarm	Attributes	Applicable major release
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.		
Remedial action: No action is required.		

Table 27-901 IK8367566

Alarm	Attributes	Applicable major release
Name: IK8367566 (10444) Type: equipmentAlarm Package: Img.IK8367566 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.		
Remedial action: No action is required.		

Table 27-902 IK8367567

Alarm	Attributes	Applicable major release
Name: IK8367567 (10445) Type: equipmentAlarm Package: Img.IK8367567 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper		
Remedial action: No action is required.		

Table 27-903 IK8367568

Alarm	Attributes	Applicable major release
Name: IK8367568 (10446) Type: equipmentAlarm Package: Img.IK8367568 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.		
Remedial action: No action is required.		

Table 27-904 IK8367569

Alarm	Attributes	Applicable major release
Name: IK8367569 (10447) Type: equipmentAlarm Package: Img.IK8367569 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.		
Remedial action: No action is required.		

Table 27-905 IK8367570

Alarm	Attributes	Applicable major release
Name: IK8367570 (10448) Type: equipmentAlarm Package: Img.IK8367570 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.		
Remedial action: No action is required.		

Table 27-906 IK8367571

Alarm	Attributes	Applicable major release
Name: IK8367571 (10449) Type: equipmentAlarm Package: Img.IK8367571 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.		
Remedial action: No action is required.		

Table 27-907 IK8367572

Alarm	Attributes	Applicable major release
Name: IK8367572 (10450) Type: equipmentAlarm Package: Img.IK8367572 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic WSMAN Major trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-907 IK8367572 (continued)

Alarm	Attributes	Applicable major release
Description: WSMAN Major trap		
Remedial action: No action is required.		

Table 27-908 IK8367573

Alarm	Attributes	Applicable major release
Name: IK8367573 (10451) Type: equipmentAlarm Package: Img.IK8367573 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic WSMAN Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Critical trap		
Remedial action: No action is required.		

Table 27-909 IK8367574

Alarm	Attributes	Applicable major release
Name: IK8367574 (10452) Type: equipmentAlarm Package: Img.IK8367574 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-910 IK8367575

Alarm	Attributes	Applicable major release
Name: IK8367575 (10453) Type: equipmentAlarm Package: Img.IK8367575 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-911 IK8367576

Alarm	Attributes	Applicable major release
Name: IK8367576 (10454) Type: equipmentAlarm Package: Img.IK8367576 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.		
Remedial action: No action is required.		

Table 27-912 IK8367577

Alarm	Attributes	Applicable major release
Name: IK8367577 (10455) Type: equipmentAlarm Package: Img.IK8367577 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-913 IK8367578

Alarm	Attributes	Applicable major release
Name: IK8367578 (10456) Type: equipmentAlarm Package: Img.IK8367578 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.		
Remedial action: No action is required.		

Table 27-914 IK8367579

Alarm	Attributes	Applicable major release
Name: IK8367579 (10457) Type: equipmentAlarm Package: Img.IK8367579 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-915 IK8367580

Alarm	Attributes	Applicable major release
Name: IK8367580 (10458) Type: equipmentAlarm Package: Img.IK8367580 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.		
Remedial action: No action is required.		

Table 27-916 IK8367581

Alarm	Attributes	Applicable major release
Name: IK8367581 (10459) Type: equipmentAlarm Package: Img.IK8367581 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.		
Remedial action: No action is required.		

Table 27-917 IK8367582

Alarm	Attributes	Applicable major release
Name: IK8367582 (10460) Type: equipmentAlarm Package: Img.IK8367582 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-918 IK8367583

Alarm	Attributes	Applicable major release
Name: IK8367583 (10461) Type: equipmentAlarm Package: Img.IK8367583 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.		

Table 27-918 IK8367583 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-919 IK8367584

Alarm	Attributes	Applicable major release
Name: IK8367584 (10462) Type: equipmentAlarm Package: lmg.IK8367584 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-920 IK8367585

Alarm	Attributes	Applicable major release
Name: IK8367585 (10463) Type: equipmentAlarm Package: lmg.IK8367585 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-921 IK8367586

Alarm	Attributes	Applicable major release
Name: IK8367586 (10464) Type: equipmentAlarm Package: lmg.IK8367586 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-922 IK8367587

Alarm	Attributes	Applicable major release
Name: IK8367587 (10465) Type: equipmentAlarm Package: Img.IK8367587 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-923 IK8367588

Alarm	Attributes	Applicable major release
Name: IK8367588 (10466) Type: equipmentAlarm Package: Img.IK8367588 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-924 IK8367589

Alarm	Attributes	Applicable major release
Name: IK8367589 (10467) Type: equipmentAlarm Package: Img.IK8367589 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-925 IK8367590

Alarm	Attributes	Applicable major release
Name: IK8367590 (10468) Type: equipmentAlarm Package: Img.IK8367590 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-926 IK8367591

Alarm	Attributes	Applicable major release
Name: IK8367591 (10469) Type: equipmentAlarm Package: Img.IK8367591 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.		
Remedial action: No action is required.		

Table 27-927 IK8367592

Alarm	Attributes	Applicable major release
Name: IK8367592 (10470) Type: equipmentAlarm Package: Img.IK8367592 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-928 IK8367593

Alarm	Attributes	Applicable major release
Name: IK8367593 (10471) Type: equipmentAlarm Package: Img.IK8367593 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-929 IK8367594

Alarm	Attributes	Applicable major release
Name: IK8367594 (10472) Type: equipmentAlarm Package: Img.IK8367594 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-929 IK8367594 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-930 IK8367595

Alarm	Attributes	Applicable major release
Name: IK8367595 (10473) Type: equipmentAlarm Package: lmg.IK8367595 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.		
Remedial action: No action is required.		

Table 27-931 IK8367596

Alarm	Attributes	Applicable major release
Name: IK8367596 (10474) Type: equipmentAlarm Package: lmg.IK8367596 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.		
Remedial action: No action is required.		

Table 27-932 IK8367597

Alarm	Attributes	Applicable major release
Name: IK8367597 (10475) Type: equipmentAlarm Package: lmg.IK8367597 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.		
Remedial action: No action is required.		

Table 27-933 IK8367598

Alarm	Attributes	Applicable major release
Name: IK8367598 (10476) Type: equipmentAlarm Package: Img.IK8367598 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.		
Remedial action: No action is required.		

Table 27-934 IK8367599

Alarm	Attributes	Applicable major release
Name: IK8367599 (10477) Type: equipmentAlarm Package: Img.IK8367599 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.		
Remedial action: No action is required.		

Table 27-935 IK8367600

Alarm	Attributes	Applicable major release
Name: IK8367600 (10478) Type: equipmentAlarm Package: Img.IK8367600 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.		
Remedial action: No action is required.		

Table 27-936 IK8367601

Alarm	Attributes	Applicable major release
Name: IK8367601 (10479) Type: equipmentAlarm Package: Img.IK8367601 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.		

Table 27-936 IK8367601 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-937 IK8367602

Alarm	Attributes	Applicable major release
Name: IK8367602 (10480) Type: equipmentAlarm Package: lmg.IK8367602 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.		
Remedial action: No action is required.		

Table 27-938 IK8367603

Alarm	Attributes	Applicable major release
Name: IK8367603 (10481) Type: equipmentAlarm Package: lmg.IK8367603 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.		
Remedial action: No action is required.		

Table 27-939 IK8367604

Alarm	Attributes	Applicable major release
Name: IK8367604 (10482) Type: equipmentAlarm Package: lmg.IK8367604 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.		
Remedial action: No action is required.		

Table 27-940 IK8367605

Alarm	Attributes	Applicable major release
Name: IK8367605 (10483) Type: equipmentAlarm Package: lmg.IK8367605 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.		
Remedial action: No action is required.		

Table 27-941 IK8367606

Alarm	Attributes	Applicable major release
Name: IK8367606 (10484) Type: equipmentAlarm Package: lmg.IK8367606 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.		
Remedial action: No action is required.		

Table 27-942 IK8367607

Alarm	Attributes	Applicable major release
Name: IK8367607 (10485) Type: equipmentAlarm Package: lmg.IK8367607 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A storage system power supply status has been set to degraded.		
Remedial action: No action is required.		

Table 27-943 IK8400982

Alarm	Attributes	Applicable major release
Name: IK8400982 (6809) Type: equipmentAlarm Package: lmg.IK8400982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG

Table 27-943 IK8400982 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-944 IK8400984

Alarm	Attributes	Applicable major release
Name: IK8400984 (6810) Type: processingErrorAlarm Package: lmg.IK8400984 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-945 IK8400986

Alarm	Attributes	Applicable major release
Name: IK8400986 (6811) Type: equipmentAlarm Package: lmg.IK8400986 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-946 IK8401008

Alarm	Attributes	Applicable major release
Name: IK8401008 (6812) Type: equipmentAlarm Package: lmg.IK8401008 Raised on class: lmg.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-947 IK8401010

Alarm	Attributes	Applicable major release
Name: IK8401010 (6813) Type: equipmentAlarm Package: Img.IK8401010 Raised on class: Img.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-948 IK8401013

Alarm	Attributes	Applicable major release
Name: IK8401013 (6814) Type: equipmentAlarm Package: Img.IK8401013 Raised on class: Img.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-949 IK8401018

Alarm	Attributes	Applicable major release
Name: IK8401018 (6815) Type: processingErrorAlarm Package: Img.IK8401018 Raised on class: Img.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-950 IK8401023

Alarm	Attributes	Applicable major release
Name: IK8401023 (6816) Type: processingErrorAlarm Package: Img.IK8401023 Raised on class: Img.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-950 IK8401023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-951 IK8401030

Alarm	Attributes	Applicable major release
Name: IK8401030 (6817) Type: equipmentAlarm Package: lmg.IK8401030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-952 IK8401033

Alarm	Attributes	Applicable major release
Name: IK8401033 (6818) Type: equipmentAlarm Package: lmg.IK8401033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-953 IK8401037

Alarm	Attributes	Applicable major release
Name: IK8401037 (6819) Type: equipmentAlarm Package: lmg.IK8401037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		

Table 27-953 IK8401037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-954 IK8401040

Alarm	Attributes	Applicable major release
Name: IK8401040 (6820) Type: environmentalAlarm Package: lmg.IK8401040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-955 IK8401060

Alarm	Attributes	Applicable major release
Name: IK8401060 (6821) Type: environmentalAlarm Package: lmg.IK8401060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-956 IK8401073

Alarm	Attributes	Applicable major release
Name: IK8401073 (6822) Type: environmentalAlarm Package: lmg.IK8401073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		

Table 27-956 IK8401073 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the Accelerator Cache Board.		

Table 27-957 IK8401091

Alarm	Attributes	Applicable major release
Name: IK8401091 (9237) Type: environmentalAlarm Package: lmg.IK8401091 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-958 IK8401098

Alarm	Attributes	Applicable major release
Name: IK8401098 (6823) Type: equipmentAlarm Package: lmg.IK8401098 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-959 IK8401102

Alarm	Attributes	Applicable major release
Name: IK8401102 (6824) Type: environmentalAlarm Package: lmg.IK8401102 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-960 IK8401105

Alarm	Attributes	Applicable major release
Name: IK8401105 (6825) Type: environmentalAlarm Package: lmg.IK8401105 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-961 IK8401112

Alarm	Attributes	Applicable major release
Name: IK8401112 (6826) Type: equipmentAlarm Package: lmg.IK8401112 Raised on class: lmg.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-962 IK8401116

Alarm	Attributes	Applicable major release
Name: IK8401116 (6827) Type: equipmentAlarm Package: lmg.IK8401116 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-963 IK8401121

Alarm	Attributes	Applicable major release
Name: IK8401121 (6828) Type: environmentalAlarm Package: lmg.IK8401121 Raised on class: lmg.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-964 IK8401125

Alarm	Attributes	Applicable major release
Name: IK8401125 (6829) Type: environmentalAlarm Package: lmg.IK8401125 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-965 IK8401129

Alarm	Attributes	Applicable major release
Name: IK8401129 (6830) Type: equipmentAlarm Package: lmg.IK8401129 Raised on class: lmg.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-966 IK8401135

Alarm	Attributes	Applicable major release
Name: IK8401135 (6831) Type: equipmentAlarm Package: lmg.IK8401135 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-966 IK8401135 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-967 IK8401144

Alarm	Attributes	Applicable major release
Name: IK8401144 (6832) Type: processingErrorAlarm Package: lmg.IK8401144 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-968 IK8401148

Alarm	Attributes	Applicable major release
Name: IK8401148 (6833) Type: equipmentAlarm Package: lmg.IK8401148 Raised on class: lmg.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-969 IK8401152

Alarm	Attributes	Applicable major release
Name: IK8401152 (6834) Type: processingErrorAlarm Package: lmg.IK8401152 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		

Table 27-969 IK8401152 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-970 IK8401154

Alarm	Attributes	Applicable major release
Name: IK8401154 (6835) Type: equipmentAlarm Package: lmg.IK8401154 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-971 IK8401156

Alarm	Attributes	Applicable major release
Name: IK8401156 (6836) Type: processingErrorAlarm Package: lmg.IK8401156 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-972 IK8401158

Alarm	Attributes	Applicable major release
Name: IK8401158 (6837) Type: processingErrorAlarm Package: lmg.IK8401158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-973 IK8401160

Alarm	Attributes	Applicable major release
Name: IK8401160 (9238) Type: communicationsAlarm Package: lmg.IK8401160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-974 IK8401163

Alarm	Attributes	Applicable major release
Name: IK8401163 (6838) Type: communicationsAlarm Package: lmg.IK8401163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-975 IK8401172

Alarm	Attributes	Applicable major release
Name: IK8401172 (6839) Type: qualityOfServiceAlarm Package: lmg.IK8401172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-976 IK8402265

Alarm	Attributes	Applicable major release
Name: IK8402265 (6840) Type: environmentalAlarm Package: lmg.IK8402265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-977 IK8402272

Alarm	Attributes	Applicable major release
Name: IK8402272 (6841) Type: environmentalAlarm Package: lmg.IK8402272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-978 IK8402279

Alarm	Attributes	Applicable major release
Name: IK8402279 (6842) Type: environmentalAlarm Package: lmg.IK8402279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-979 IK8402291

Alarm	Attributes	Applicable major release
Name: IK8402291 (6843) Type: equipmentAlarm Package: lmg.IK8402291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-980 IK8402292

Alarm	Attributes	Applicable major release
Name: IK8402292 (6844) Type: environmentalAlarm Package: lmg.IK8402292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-981 IK8402295

Alarm	Attributes	Applicable major release
Name: IK8402295 (6845) Type: equipmentAlarm Package: lmg.IK8402295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-982 IK8402302

Alarm	Attributes	Applicable major release
Name: IK8402302 (6846) Type: equipmentAlarm Package: lmg.IK8402302 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-983 IK8402337

Alarm	Attributes	Applicable major release
Name: IK8402337 (6847) Type: communicationsAlarm Package: lmg.IK8402337 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-984 IK8402341

Alarm	Attributes	Applicable major release
Name: IK8402341 (6848) Type: communicationsAlarm Package: lmg.IK8402341 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-985 IK8402343

Alarm	Attributes	Applicable major release
Name: IK8402343 (6849) Type: communicationsAlarm Package: lmg.IK8402343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-986 IK8402347

Alarm	Attributes	Applicable major release
Name: IK8402347 (6850) Type: communicationsAlarm Package: lmg.IK8402347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-987 IK8402349

Alarm	Attributes	Applicable major release
Name: IK8402349 (6851) Type: communicationsAlarm Package: lmg.IK8402349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-988 IK8402360

Alarm	Attributes	Applicable major release
Name: IK8402360 (6852) Type: equipmentAlarm Package: lmg.IK8402360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-989 IK8402363

Alarm	Attributes	Applicable major release
Name: IK8402363 (6853) Type: environmentalAlarm Package: lmg.IK8402363 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-990 IK8402368

Alarm	Attributes	Applicable major release
Name: IK8402368 (6854) Type: equipmentAlarm Package: lmg.IK8402368 Raised on class: lmg.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-991 IK8402369

Alarm	Attributes	Applicable major release
Name: IK8402369 (6855) Type: equipmentAlarm Package: Img.IK8402369 Raised on class: Img.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-992 IK8402374

Alarm	Attributes	Applicable major release
Name: IK8402374 (6856) Type: equipmentAlarm Package: Img.IK8402374 Raised on class: Img.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-993 IK8402375

Alarm	Attributes	Applicable major release
Name: IK8402375 (6857) Type: equipmentAlarm Package: Img.IK8402375 Raised on class: Img.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-994 IK8402376

Alarm	Attributes	Applicable major release
Name: IK8402376 (6858) Type: equipmentAlarm Package: lmg.IK8402376 Raised on class: lmg.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-995 IK8402377

Alarm	Attributes	Applicable major release
Name: IK8402377 (6859) Type: equipmentAlarm Package: lmg.IK8402377 Raised on class: lmg.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-996 IK8402378

Alarm	Attributes	Applicable major release
Name: IK8402378 (6860) Type: equipmentAlarm Package: lmg.IK8402378 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-997 IK8402379

Alarm	Attributes	Applicable major release
Name: IK8402379 (6861) Type: equipmentAlarm Package: Img.IK8402379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-998 IK8402380

Alarm	Attributes	Applicable major release
Name: IK8402380 (6862) Type: equipmentAlarm Package: Img.IK8402380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-999 IK8402382

Alarm	Attributes	Applicable major release
Name: IK8402382 (6863) Type: environmentalAlarm Package: Img.IK8402382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-1000 IK8402386

Alarm	Attributes	Applicable major release
Name: IK8402386 (6864) Type: equipmentAlarm Package: lmg.IK8402386 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1001 IK8402387

Alarm	Attributes	Applicable major release
Name: IK8402387 (6865) Type: equipmentAlarm Package: lmg.IK8402387 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1002 IK8402388

Alarm	Attributes	Applicable major release
Name: IK8402388 (6866) Type: equipmentAlarm Package: lmg.IK8402388 Raised on class: lmg.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1003 IK8402391

Alarm	Attributes	Applicable major release
Name: IK8402391 (6867) Type: processingErrorAlarm Package: Img.IK8402391 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-1004 IK8402401

Alarm	Attributes	Applicable major release
Name: IK8402401 (6868) Type: communicationsAlarm Package: Img.IK8402401 Raised on class: Img.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-1005 IK8402408

Alarm	Attributes	Applicable major release
Name: IK8402408 (6869) Type: qualityOfServiceAlarm Package: Img.IK8402408 Raised on class: Img.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1006 IK8402409

Alarm	Attributes	Applicable major release
Name: IK8402409 (6870) Type: processingErrorAlarm Package: lmg.IK8402409 Raised on class: lmg.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1007 IK8402411

Alarm	Attributes	Applicable major release
Name: IK8402411 (6871) Type: equipmentAlarm Package: lmg.IK8402411 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1008 IK8402428

Alarm	Attributes	Applicable major release
Name: IK8402428 (6872) Type: equipmentAlarm Package: lmg.IK8402428 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1009 IK8402429

Alarm	Attributes	Applicable major release
Name: IK8402429 (6873) Type: equipmentAlarm Package: lmg.IK8402429 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		

Table 27-1009 IK8402429 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1010 IK8402431

Alarm	Attributes	Applicable major release
Name: IK8402431 (6874) Type: equipmentAlarm Package: lmg.IK8402431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1011 IK8402432

Alarm	Attributes	Applicable major release
Name: IK8402432 (6875) Type: equipmentAlarm Package: lmg.IK8402432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1012 IK8402436

Alarm	Attributes	Applicable major release
Name: IK8402436 (6876) Type: equipmentAlarm Package: lmg.IK8402436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1013 IK8402437

Alarm	Attributes	Applicable major release
Name: IK8402437 (6877) Type: equipmentAlarm Package: lmg.IK8402437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1014 IK8402439

Alarm	Attributes	Applicable major release
Name: IK8402439 (6878) Type: communicationsAlarm Package: lmg.IK8402439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1015 IK8402559

Alarm	Attributes	Applicable major release
Name: IK8402559 (6879) Type: equipmentAlarm Package: lmg.IK8402559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-1016 IK8402609

Alarm	Attributes	Applicable major release
Name: IK8402609 (6880) Type: processingErrorAlarm Package: lmg.IK8402609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-1016 IK8402609 (continued)

Alarm	Attributes	Applicable major release
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1017 IK8402610

Alarm	Attributes	Applicable major release
Name: IK8402610 (6881) Type: processingErrorAlarm Package: lmg.IK8402610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1018 IK8402615

Alarm	Attributes	Applicable major release
Name: IK8402615 (6882) Type: equipmentAlarm Package: lmg.IK8402615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-1019 IK8402616

Alarm	Attributes	Applicable major release
Name: IK8402616 (6883) Type: environmentalAlarm Package: lmg.IK8402616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-1020 IK8402617

Alarm	Attributes	Applicable major release
Name: IK8402617 (6884) Type: environmentalAlarm Package: lmg.IK8402617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-1021 IK8402620

Alarm	Attributes	Applicable major release
Name: IK8402620 (6885) Type: equipmentAlarm Package: lmg.IK8402620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-1022 IK8402622

Alarm	Attributes	Applicable major release
Name: IK8402622 (6886) Type: environmentalAlarm Package: Img.IK8402622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-1023 IK8402628

Alarm	Attributes	Applicable major release
Name: IK8402628 (6887) Type: equipmentAlarm Package: Img.IK8402628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-1024 IK8402632

Alarm	Attributes	Applicable major release
Name: IK8402632 (6888) Type: processingErrorAlarm Package: Img.IK8402632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1025 IK8402633

Alarm	Attributes	Applicable major release
Name: IK8402633 (6889) Type: communicationsAlarm Package: lmg.IK8402633 Raised on class: lmg.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-1026 IK8402636

Alarm	Attributes	Applicable major release
Name: IK8402636 (9239) Type: equipmentAlarm Package: lmg.IK8402636 Raised on class: lmg.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1027 IK8402648

Alarm	Attributes	Applicable major release
Name: IK8402648 (6890) Type: qualityOfServiceAlarm Package: lmg.IK8402648 Raised on class: lmg.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1028 IK8402657

Alarm	Attributes	Applicable major release
Name: IK8402657 (6891) Type: environmentalAlarm Package: lmg.IK8402657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1029 IK8404762

Alarm	Attributes	Applicable major release
Name: IK8404762 (6892) Type: communicationsAlarm Package: lmg.IK8404762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1030 IK8450919

Alarm	Attributes	Applicable major release
Name: IK8450919 (9240) Type: communicationsAlarm Package: lmg.IK8450919 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwDefGwDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwDefGwDown alarm signifies that the default gateway is down.\nAlarm is cleared by the system.\nReason: bt2SwDefGwDown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1031 IK8450921

Alarm	Attributes	Applicable major release
Name: IK8450921 (9241) Type: processingErrorAlarm Package: lmg.IK8450921 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwDefGwNotInService Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwDefGwDisabled alarm signifies that the default gateway is alive but not in service.\nAlarm is cleared by the system.\nReason: bt2SwDefGwNotInService		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1032 IK8450931

Alarm	Attributes	Applicable major release
Name: IK8450931 (6893) Type: processingErrorAlarm Package: lmg.IK8450931 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwFwDownloadFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG
Description: A bt2SwFwDownloadFailure signifies that firmware downloaded failed to [image1|image2|boot image].\nAlarm is cleared by the system.\nReason: bt2SwFwDownloadFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1033 IK8450935

Alarm	Attributes	Applicable major release
Name: IK8450935 (9242) Type: communicationsAlarm Package: lmg.IK8450935 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwUfdfoLtMFailure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwUfdfoLtMFailure alarm signifies that a LtM link is down.\nAlarm is cleared by the system.\nReason: bt2SwUfdfoLtMFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1034 IK8450938

Alarm	Attributes	Applicable major release
Name: IK8450938 (9243) Type: processingErrorAlarm Package: lmg.IK8450938 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwUfdfoGlobalDis Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG

Table 27-1034 IK8450938 (continued)

Alarm	Attributes	Applicable major release
Description: A bt2SwUfdfoGlobalDis alarm signifies that Global UFD is disabled.\nAlarm is cleared by the system.\nReason: bt2SwUfdfoGlobalDis		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1035 IK8450940

Alarm	Attributes	Applicable major release
Name: IK8450940 (9244) Type: communicationsAlarm Package: lmg.IK8450940 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwUfdfoLtDAutoDis Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwUfdfoLtDAutoDis alarm signifies that a LtD link is Auto Disabled.\nAlarm is cleared by the system.\nReason: bt2SwUfdfoLtDAutoDis		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1036 IK8450948

Alarm	Attributes	Applicable major release
Name: IK8450948 (9245) Type: communicationsAlarm Package: lmg.IK8450948 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwHotlinksMasterDn Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwHotlinksMasterDn alarm signifies that the Master interface is not active.\nAlarm is cleared by the system.\nReason: bt2SwHotlinksMasterDn		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1037 IK8450950

Alarm	Attributes	Applicable major release
Name: IK8450950 (9246) Type: communicationsAlarm Package: lmg.IK8450950 Raised on class: lmg.FRU	Severity: major Specific problem: bt2SwHotlinksBackupDn Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bt2SwHotlinksBackupDn alarm signifies that the Backup interface is not active.\nAlarm is cleared by the system.\nReason: bt2SwHotlinksBackupDn		

Table 27-1037 IK8450950 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1038 IK8450959

Alarm	Attributes	Applicable major release
Name: IK8450959 (6894) Type: communicationsAlarm Package: lmg.IK8450959 Raised on class: lmg.FRU	Severity: major Specific problem: The switch has failed a TFTP transfer Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The switch has failed a TFTP transfer.\nAlarm is cleared by the system.\nReason: switchTFTPTransferFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1039 IK8450961

Alarm	Attributes	Applicable major release
Name: IK8450961 (6895) Type: environmentalAlarm Package: lmg.IK8450961 Raised on class: lmg.FRU	Severity: major Specific problem: The switch fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The switch fan has failed.\nAlarm is cleared by the system.\nReason: switchFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1040 IK8450963

Alarm	Attributes	Applicable major release
Name: IK8450963 (6896) Type: environmentalAlarm Package: lmg.IK8450963 Raised on class: lmg.FRU	Severity: major Specific problem: switchTempSensorDegraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The switch temperature sensor indicates a high temperature condition.\nAlarm is cleared by the system.\nReason: switchTempSensorDegraded		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1041 IK8450964

Alarm	Attributes	Applicable major release
Name: IK8450964 (9247) Type: environmentalAlarm Package: Img.IK8450964 Raised on class: Img.FRU	Severity: critical Specific problem: switchTempSensorFailed Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The switch temperature sensor indicates an over-temperature condition.\nAlarm is cleared by the system.\nReason: switchTempSensorFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1042 IK8450971

Alarm	Attributes	Applicable major release
Name: IK8450971 (6897) Type: equipmentAlarm Package: Img.IK8450971 Raised on class: Img.LMGMngElement	Severity: major Specific problem: overheat Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A overheat alarm indicates that the on board temperature sensor has reported a overheat condition. System will shutdown until unit has sufficiently cooled such that operation may begin again. A cold start alarm will be issued when the unit has come back on line.\nAlarm to be cleared by the operator at the management system.\nReason: overheat		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1043 IK8450975

Alarm	Attributes	Applicable major release
Name: IK8450975 (6898) Type: equipmentAlarm Package: Img.IK8450975 Raised on class: Img.FRU	Severity: major Specific problem: powerSupplyFail Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One or more sources of power to this agent has failed. Presumably a redundant power-supply has taken over.\nAlarm is cleared by the system.\nReason: powerSupplyFail		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1044 IK8450977

Alarm	Attributes	Applicable major release
Name: IK8450977 (6899) Type: equipmentAlarm Package: lmg.IK8450977 Raised on class: lmg.FRU	Severity: major Specific problem: rpsAlrm Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Attached Redundant Power Supply device is indicating an alarm condition.\nAlarm is cleared by the system.\nReason: rpsAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1045 IK8450982

Alarm	Attributes	Applicable major release
Name: IK8450982 (6900) Type: equipmentAlarm Package: lmg.IK8450982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-1046 IK8450984

Alarm	Attributes	Applicable major release
Name: IK8450984 (6901) Type: processingErrorAlarm Package: lmg.IK8450984 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-1047 IK8450986

Alarm	Attributes	Applicable major release
Name: IK8450986 (6902) Type: equipmentAlarm Package: Img.IK8450986 Raised on class: Img.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-1048 IK8451008

Alarm	Attributes	Applicable major release
Name: IK8451008 (6903) Type: equipmentAlarm Package: Img.IK8451008 Raised on class: Img.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-1049 IK8451010

Alarm	Attributes	Applicable major release
Name: IK8451010 (6904) Type: equipmentAlarm Package: Img.IK8451010 Raised on class: Img.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-1050 IK8451013

Alarm	Attributes	Applicable major release
Name: IK8451013 (6905) Type: equipmentAlarm Package: lmg.IK8451013 Raised on class: lmg.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-1051 IK8451018

Alarm	Attributes	Applicable major release
Name: IK8451018 (6906) Type: processingErrorAlarm Package: lmg.IK8451018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-1052 IK8451023

Alarm	Attributes	Applicable major release
Name: IK8451023 (6907) Type: processingErrorAlarm Package: lmg.IK8451023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-1053 IK8451030

Alarm	Attributes	Applicable major release
Name: IK8451030 (6908) Type: equipmentAlarm Package: lmg.IK8451030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-1053 IK8451030 (continued)

Alarm	Attributes	Applicable major release
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-1054 IK8451033

Alarm	Attributes	Applicable major release
Name: IK8451033 (6909) Type: equipmentAlarm Package: lmg.IK8451033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-1055 IK8451037

Alarm	Attributes	Applicable major release
Name: IK8451037 (6910) Type: equipmentAlarm Package: lmg.IK8451037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-1056 IK8451040

Alarm	Attributes	Applicable major release
Name: IK8451040 (6911) Type: environmentalAlarm Package: lmg.IK8451040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1056 IK8451040 (continued)

Alarm	Attributes	Applicable major release
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabTemperatureCriti-calTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-1057 IK8451042

Alarm	Attributes	Applicable major release
Name: IK8451042 (6912) Type: equipmentAlarm Package: Img.IK8451042 Raised on class: Img.FRU	Severity: major Specific problem: High Priority Alert Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A high priority alert has occurred.\nAlarm is cleared by the system when the device is restarted.\nReason: trapDceoHighPriority		
Remedial action: Check the Trap Details for more information.		

Table 27-1058 IK8451052

Alarm	Attributes	Applicable major release
Name: IK8451052 (6913) Type: equipmentAlarm Package: Img.IK8451052 Raised on class: Img.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system when the device is restarted.\nReason: trapDscCritical		
Remedial action: Check the Trap Description for more information.		

Table 27-1059 IK8451060

Alarm	Attributes	Applicable major release
Name: IK8451060 (6914) Type: environmentalAlarm Package: Img.IK8451060 Raised on class: Img.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1060 IK8451073

Alarm	Attributes	Applicable major release
Name: IK8451073 (6915) Type: environmentalAlarm Package: Img.IK8451073 Raised on class: Img.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1061 IK8451091

Alarm	Attributes	Applicable major release
Name: IK8451091 (9248) Type: environmentalAlarm Package: Img.IK8451091 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1062 IK8451098

Alarm	Attributes	Applicable major release
Name: IK8451098 (6916) Type: equipmentAlarm Package: Img.IK8451098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-1063 IK8451102

Alarm	Attributes	Applicable major release
Name: IK8451102 (6917) Type: environmentalAlarm Package: lmg.IK8451102 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1064 IK8451105

Alarm	Attributes	Applicable major release
Name: IK8451105 (6918) Type: environmentalAlarm Package: lmg.IK8451105 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1065 IK8451112

Alarm	Attributes	Applicable major release
Name: IK8451112 (6919) Type: equipmentAlarm Package: lmg.IK8451112 Raised on class: lmg.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-1066 IK8451116

Alarm	Attributes	Applicable major release
Name: IK8451116 (6920) Type: equipmentAlarm Package: Img.IK8451116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1067 IK8451121

Alarm	Attributes	Applicable major release
Name: IK8451121 (6921) Type: environmentalAlarm Package: Img.IK8451121 Raised on class: Img.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1068 IK8451125

Alarm	Attributes	Applicable major release
Name: IK8451125 (6922) Type: environmentalAlarm Package: Img.IK8451125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1069 IK8451129

Alarm	Attributes	Applicable major release
Name: IK8451129 (6923) Type: equipmentAlarm Package: Img.IK8451129 Raised on class: Img.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-1069 IK8451129 (continued)

Alarm	Attributes	Applicable major release
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-1070 IK8451135

Alarm	Attributes	Applicable major release
Name: IK8451135 (6924) Type: equipmentAlarm Package: Img.IK8451135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1071 IK8451144

Alarm	Attributes	Applicable major release
Name: IK8451144 (6925) Type: processingErrorAlarm Package: Img.IK8451144 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-1072 IK8451148

Alarm	Attributes	Applicable major release
Name: IK8451148 (6926) Type: equipmentAlarm Package: Img.IK8451148 Raised on class: Img.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-1073 IK8451152

Alarm	Attributes	Applicable major release
Name: IK8451152 (6927) Type: processingErrorAlarm Package: Img.IK8451152 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-1074 IK8451154

Alarm	Attributes	Applicable major release
Name: IK8451154 (6928) Type: equipmentAlarm Package: Img.IK8451154 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-1075 IK8451156

Alarm	Attributes	Applicable major release
Name: IK8451156 (6929) Type: processingErrorAlarm Package: Img.IK8451156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1076 IK8451158

Alarm	Attributes	Applicable major release
Name: IK8451158 (6930) Type: processingErrorAlarm Package: lmg.IK8451158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1077 IK8451160

Alarm	Attributes	Applicable major release
Name: IK8451160 (9249) Type: communicationsAlarm Package: lmg.IK8451160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-1078 IK8451163

Alarm	Attributes	Applicable major release
Name: IK8451163 (6931) Type: communicationsAlarm Package: lmg.IK8451163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-1079 IK8451172

Alarm	Attributes	Applicable major release
Name: IK8451172 (6932) Type: qualityOfServiceAlarm Package: lmg.IK8451172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1080 IK8451182

Alarm	Attributes	Applicable major release
Name: IK8451182 (6933) Type: processingErrorAlarm Package: lmg.IK8451182 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: softwareProgramError	Release: • LR14.3.MG
Description: The physical disk drive identified by the device field has been rendered inoperable. If the flags.quorum_disk flag is nonzero, the physical disk drive is the Storage System Quorum disk identified in the quorum_sequence field. . If the flags.inq_state flag is nonzero, the content of the inq_data and capacity fields is valid. . If the rss_flags.member_abnormal flag is nonzero, the content of the member_state field is valid. . The rack_num field will not be valid until a future release. The reason_code field contains a code giving the reason the physical disk drive has been rendered inoperable: . 0x001 =" CS IO failure . 0x002 = Scrubber IO failure . 0x003 = Attempt to set CBIT on normal drive . 0x004 = Attempt to set CBIT on merging drive . 0x100 = The Target Discovery Service Descriptor retry count has been exceeded . 0x101 = Inoperable for Bad Block Replacement . 0x102 = The soft error count has been exceeded . 0x103 = The number of exchange timeouts permitted was exceeded . 0x104 = Communication with drive has failed an excessive number of times . 0x105 = The number of retries has been exceeded . 0x106 = Medium/Hardware Errors encountered on this physical disk drive . 0x107 = The number of Directed LIP's has surpassed the threshold . 0x200 = Smart event from a physical disk drive not in Storage System . 0x201 = Smart event from a physical disk drive not a Volume . 0x202 = Smart event from a physical disk drive not a RSS . 0x203 = Failure predicted from physical disk drive . 0x204 = Can't read from physical disk drive from the poll . 0x205 = Failure predicted from physical disk drive while deleting Disk Group . 0x206 = physical disk drive forced inoperative from maintenance command for temporary POID . 0x207 = physical disk drive forced inoperative from maintenance command for POID . 0x208 = Bad block recovery failed or can't read FPAB . 0x209 = Failure to remove volume from Storage System . 0x20A = Failure to update metadata .\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_3_1"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1081 IK8451192

Alarm	Attributes	Applicable major release
Name: IK8451192 (6934) Type: processingErrorAlarm Package: lmg.IK8451192 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG

Table 27-1081 IK8451192 (continued)

Alarm	Attributes	Applicable major release
Description: A machine check occurred while a termination event was being processed. The post-termination operation being performed at the time the event occurred can be derived from the Iter.reuea_index field. Note: The Iteihd and Iter fields may not describe the event that caused the HSV110 controller to terminate operation depending on how far termination processing got before the machine check occurred.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_4_2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1082 IK8451202

Alarm	Attributes	Applicable major release
Name: IK8451202 (6935) Type: equipmentAlarm Package: lmg.IK8451202 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Fault Manager on the Storage System Master received an invalid Event Information Packet from the remote Fault Manager. The header information from the invalid Event Information Packet is contained in the ainfo.remote_event field. Note: The content of the ainfo.quiesce_type field, ainfo.events_not_reported field, cinfo.scelcbi structure, cinfo.sctelcbi structure, minfo.scelmi structure, and minfo.sctelmi structure is undefined.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_4_c		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1083 IK8451208

Alarm	Attributes	Applicable major release
Name: IK8451208 (6936) Type: equipmentAlarm Package: lmg.IK8451208 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1083 IK8451208 (continued)

Alarm	Attributes	Applicable major release
Description: A physical disk drive has reported that it has exceeded its failure prediction threshold. The identity of the physical disk drive is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The arbitrated loop physical address of the physical disk drive is contained in the al_pa field. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. The Fibre Channel Exchange Descriptor class is contained in the fed_class field. The command issued to the physical disk drive is contained in the cmd field. The sense data obtained from the physical disk drive as a result of the failure prediction threshold exceeded error is contained in the error field. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_0		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1084 IK8451216

Alarm	Attributes	Applicable major release
Name: IK8451216 (6937) Type: equipmentAlarm Package: lmg.IK8451216 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1084 IK8451216 (continued)

Alarm	Attributes	Applicable major release
Description: A physical disk drive has reported numerous failure prediction threshold exceeded errors. The identity of the physical disk drive is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The arbitrated loop physical address of the physical disk drive is contained in the al_pa field. The missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. The Fibre Channel Exchange Descriptor class is contained in the fed_class field. The num_times field is the number of failure prediction threshold exceeded errors reported by the physical disk drive in the previous minute. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_9		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1085 IK8451221

Alarm	Attributes	Applicable major release
Name: IK8451221 (6938) Type: equipmentAlarm Package: lmg.IK8451221 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A Drive Enclosure Environmental Monitoring Unit requested a code update but the code update could not be found, so the update was not performed. The identity of the affected Drive Enclosure Environmental Monitoring Unit is contained in the device field. The Fibre Channel port used to communicate with the Drive Enclosure Environmental Monitoring Unit is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the Drive Enclosure Environmental Monitoring Unit is contained in the port field. The missing_port and missing_cerp_id fields are unused. The location of the Drive Enclosure Environmental Monitoring Unit is contained in the rack_num and dencl_num fields. Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the al_pa, bay, fed_class and num_times field is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_e		

Table 27-1085 IK8451221 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1086 IK8451222

Alarm	Attributes	Applicable major release
Name: IK8451222 (6939) Type: equipmentAlarm Package: lmg.IK8451222 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Drive Enclosure Environmental Monitoring Unit is able to communicate with a physical disk drive but this HSV110 controller is unable to communicate with that physical disk drive on the Fibre Channel bus. The identity of the Drive Enclosure Environmental Monitoring Unit is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is contained in the rack_num, dencl_num, and bay fields. Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the al_pa, fed_class and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_f		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1087 IK8451226

Alarm	Attributes	Applicable major release
Name: IK8451226 (6940) Type: equipmentAlarm Package: lmg.IK8451226 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1087 IK8451226 (continued)

Alarm	Attributes	Applicable major release
Description: There are too many drive enclosures attached to a Fibre Channel port. The Fibre Channel port with too many drive enclosures attached to the HSV110 controller is contained in the cerp_id field. Note that in this case the content of the bay, fed_class, rack_num, dencl_num and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The missing_port and missing_cerp_id fields are unused. The location of the identified in the cerp_id field. The device, missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_14		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1088 IK8451227

Alarm	Attributes	Applicable major release
Name: IK8451227 (6941) Type: communicationsAlarm Package: lmg.IK8451227 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The cable connected to the I/O module is attached to the wrong Fibre Channel port. The Fibre Channel port incorrectly attached to the HSV110 controller is contained in the cerp_id field. Note that in this case the content of the device, missing_port, missing_cerp_id, bay, fed_class, rack_num, dencl_num and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_15		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1089 IK8451228

Alarm	Attributes	Applicable major release
Name: IK8451228 (6942) Type: equipmentAlarm Package: lmg.IK8451228 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1089 IK8451228 (continued)

Alarm	Attributes	Applicable major release
Description: A HSV110 controller does not have an address on the enclosure address bus. The HSV110 controller location cannot be identified. Note that in this case the content of the missing_port, missing_cerp_id, bay, fed_class, rack_num, dencl_num, al_pa, device, cerp_id, port, enclosures array and num_times fields is undefined.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_16		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1090 IK8451231

Alarm	Attributes	Applicable major release
Name: IK8451231 (6943) Type: equipmentAlarm Package: lmg.IK8451231 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A physical disk drive has exceeded its soft error threshold. The identity of the physical disk drive is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The arbitrated loop physical address of the physical disk drive is contained in the al_pa field. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class, cdb, and sense_data fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_1a		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1091 IK8451235

Alarm	Attributes	Applicable major release
Name: IK8451235 (6944) Type: equipmentAlarm Package: lmg.IK8451235 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1091 IK8451235 (continued)

Alarm	Attributes	Applicable major release
Description: A HSV110 controller has detected only one port of a Fibre Channel device. This Fibre Channel device has entered the Single Port on Fibre state which should be corrected as soon as possible. The identity of the Fibre Channel device is contained in the device field. The Fibre Channel port still able to communicate with the Fibre Channel device is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number able to communicate with the Fibre Channel device is contained in the port field. The Fibre Channel port unable to communicate with the Fibre Channel device is contained in the missing_cerp_id field. The HSV110 controller internal Fibre Channel port number unable to communicate with the Fibre Channel device is contained in the missing_port field. The arbitrated loop physical address of the Fibre Channel device is contained in the al_pa field. The location of the Fibre Channel device is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class, and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_1e		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1092 IK8451237

Alarm	Attributes	Applicable major release
Name: IK8451237 (6945) Type: equipmentAlarm Package: lmg.IK8451237 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1092 IK8451237 (continued)

Alarm	Attributes	Applicable major release
Description: An unsupported Fibre Channel device has been detected. The drive has been failed to prevent possible data corruption or system instability. The identity of the Fibre Channel device is contained in the device field. The Fibre Channel port used to communicate with the Fibre Channel device is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the Fibre Channel device is contained in the port field. The arbitrated loop physical address of the Fibre Channel device is contained in the al_pa field. The missing_port and missing_cerp_id fields are unused. The location of the Fibre Channel device is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_20		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1093 IK8451241

Alarm	Attributes	Applicable major release
Name: IK8451241 (6946) Type: equipmentAlarm Package: Img.IK8451241 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1093 IK8451241 (continued)

Alarm	Attributes	Applicable major release
Description: A Drive Enclosure Environmental Monitoring Unit has failed to assign a hard address to a physical disk drive on the loop. The device field contains the identity of the enclosure. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The al_pa field contains the expected AL_PA, and the num_times field contains the actual AL_PA. The missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note that in this case the content of the fed_class is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_25		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1094 IK8451242

Alarm	Attributes	Applicable major release
Name: IK8451242 (6947) Type: equipmentAlarm Package: lmg.IK8451242 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1094 IK8451242 (continued)

Alarm	Attributes	Applicable major release
Description: A Drive Enclosure Environmental Monitoring Unit has failed to assign an address to a physical disk drive on the loop. This has occurred because another physical disk drive has already obtained this AL_PA. The device field contains the identity of the enclosure. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The al_pa field contains the AL_PA that was stolen. The missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_26		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1095 IK8451243

Alarm	Attributes	Applicable major release
Name: IK8451243 (6948) Type: equipmentAlarm Package: Img.IK8451243 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1095 IK8451243 (continued)

Alarm	Attributes	Applicable major release
Description: A Drive Enclosure Environmental Monitoring Unit has failed to assign address(s) to a physical disk drive on the loop. Soft addressing was detected for this enclosure. The device field contains the identity of the enclosure. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The missing_port and missing_cerp_id fields are unused. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class, al_pa, and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_27		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1096 IK8451247

Alarm	Attributes	Applicable major release
Name: IK8451247 (6949) Type: equipmentAlarm Package: lmg.IK8451247 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A physical disk drive was bypassed rendering it unusable. The physical disk drive is unusable because a Drive Enclosure Environmental Monitoring Unit bypassed a drive bay or the physical disk drive left itself bypassed. The physical disk drive is not available to the HSV110 controllers and will not be displayed by the HSV element manager GUI. The physical disk drive fault led will be lit to indicate that it is unusable. The Fibre Channel port over which this condition was detected is identified in the cerp_id field. The HSV110 controller internal Fibre Channel port over which this condition was detected is contained in the port field. The al_pa field is invalid. The location of the physical disk drive is as indicated by the content of the rack_num, dencl_num, and bay fields. Note that the content of the rack_num field will not be valid until a future release. The bypass_reason field is used to indicate how the physical disk drive was bypassed: . 1 =" The physical disk drive left itself bypassed . 2 = The Drive Enclosure Environmental Monitoring Unit bypassed the drive bay . The Drive Enclosure Environmental Monitoring Unit is identified in the device field. Additionally, the content of the pid, rev, and enclosures array fields is undefined in this case.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_2b"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1097 IK8451251

Alarm	Attributes	Applicable major release
Name: IK8451251 (6950) Type: equipmentAlarm Package: lmg.IK8451251 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A HSV110 controller has detected only one port of all Fibre Channel devices in an enclosure. These Fibre Channel devices have entered the Single Port on Fibre state which should be corrected as soon as possible. The identity of the Fibre Channel device enclosure is contained in the device field. The Fibre Channel port still able to communicate with the Fibre Channel device is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number able to communicate with the Fibre Channel device is contained in the port field. The Fibre Channel port unable to communicate with the Fibre Channel device is contained in the missing_cerp_id field. The HSV110 controller internal Fibre Channel port number unable to communicate with the Fibre Channel device is contained in the missing_port field. The al_pa and bay fields are invalid. The location of the Fibre Channel enclosure is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. Note also that in this case the content of the fed_class, and num_times fields is undefined. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_30		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1098 IK8451253

Alarm	Attributes	Applicable major release
Name: IK8451253 (6951) Type: communicationsAlarm Package: lmg.IK8451253 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A HSV110 controller has detected only one port of all Fibre Channel devices on a loop. These Fibre Channel devices have entered the Single Port on Fibre state which should be corrected as soon as possible. The device, al_pa, dencl_num, and bay fields are all invalid. The Fibre Channel port still able to communicate with the Fibre Channel device is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number able to communicate with the Fibre Channel device is contained in the port field. The Fibre Channel port unable to communicate with the Fibre Channel device is contained in the missing_cerp_id field. The HSV110 controller internal Fibre Channel port number unable to communicate with the Fibre Channel device is contained in the missing_port field.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_32		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1099 IK8451256

Alarm	Attributes	Applicable major release
Name: IK8451256 (6952) Type: equipmentAlarm Package: lmg.IK8451256 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: An unrecognized Fibre Channel physical disk drive firmware revision has been detected by the physical disk drive firmware load process. The identity of the physical disk drive is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The arbitrated loop physical address of the physical disk drive is contained in the al_pa field. The bypass_reason field is invalid. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num, al_pa and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. The pid field contains the SCSI Inquiry Product Identification obtained from the physical disk drive. The rev field contains the current firmware revision obtained from the physical disk drive. The new_rev field contains the latest firmware version known to the controller, or blanks if the isn't a known version. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_35		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1100 IK8451257

Alarm	Attributes	Applicable major release
Name: IK8451257 (6953) Type: equipmentAlarm Package: lmg.IK8451257 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1100 IK8451257 (continued)

Alarm	Attributes	Applicable major release
Description: An unsupported Fibre Channel physical disk drive firmware revision has been detected by the physical disk drive firmware load process. The identity of the physical disk drive is contained in the device field. The Fibre Channel port used to communicate with the physical disk drive is contained in the cerp_id field. The HSV110 controller internal Fibre Channel port number used to communicate with the physical disk drive is contained in the port field. The arbitrated loop physical address of the physical disk drive is contained in the al_pa field. The bypass_reason field is invalid. The location of the physical disk drive is determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num, dencl_num, and bay fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num, al_pa and bay fields is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num, dencl_num, and bay fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. The identity contained in the device field should be used to confirm the last known location values. . Note that the content of the rack_num field will not be valid until a future release. The pid field contains the SCSI Inquiry Product Identification obtained from the physical disk drive. The rev field contains the current firmware revision obtained from the physical disk drive. The new_rev field contains the latest firmware version known to the controller, or blanks if the isn't a known version. The enclosures array shows the drive enclosures available on the Fibre Channel port identified in the cerp_id field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_36		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1101 IK8451265

Alarm	Attributes	Applicable major release
Name: IK8451265 (6954) Type: equipmentAlarm Package: lmg.IK8451265 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The HSV110 controller has detected an enclosure on the Fibre Channel but is unable to communicate with the EMU on the CAB bus or the EMU is reporting an invalid enclosure number. All fields except port and rack are invalid. other fields are invalid.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_6_3e		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1102 IK8451287

Alarm	Attributes	Applicable major release
Name: IK8451287 (6955) Type: environmentalAlarm Package: lmg.IK8451287 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG

Table 27-1102 IK8451287 (continued)

Alarm	Attributes	Applicable major release
Description: The temperature trip point for a temperature sensor located within an HSV110 controller has been reached. The HSV110 controller is identified in the handle field. The value.ul1 field contains the current temperature reading from I2C sensor 1 in degrees celsius while the value.ul2 field contains the adjusted reading from I2C sensor 2. The set temperature trip point is contained in the secondary_id field.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_e		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1103 IK8451290

Alarm	Attributes	Applicable major release
Name: IK8451290 (6956) Type: equipmentAlarm Package: lmg.IK8451290 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The '1' blower located within the HSV110 controller identified in the handle field is running slower than the lowest acceptable speed. The secondary_id field contains the '1' blower assembly internal identifier value: 1. The value.ul1 field contains the current speed of the '1' blower. The value.ul2 field contains the lowest acceptable speed for the '1' blower.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_12		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1104 IK8451295

Alarm	Attributes	Applicable major release
Name: IK8451295 (6957) Type: environmentalAlarm Package: lmg.IK8451295 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: An HSV110 controller's battery assembly has been removed. The Battery Present flag for battery assembly '1' located within the HSV110 controller identified in the handle field has changed from PRESENT to NOT PRESENT indicating that the battery assembly was removed. The secondary_id field contains the battery assembly '1' internal identifier value: 1. The value.ul1 field contains the new state of the Battery Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Battery Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_17		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1105 IK8451301

Alarm	Attributes	Applicable major release
Name: IK8451301 (6958) Type: environmentalAlarm Package: lmg.IK8451301 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: An HSV110 controller's battery assembly has malfunctioned. The Battery In Use flag for battery assembly '1' located within the HSV110 controller identified in the handle field has transitioned from the IN USE to NOT IN USE state indicating that the battery assembly has malfunctioned. The secondary_id field contains the battery assembly '1' internal identifier value: 1. The value.ul1 field contains the new state of the Battery In Use flag: 0 (NOT IN USE). The value.ul2 field contains the old state of the Battery In Use flag: 1 (IN USE).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_1d		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1106 IK8451303

Alarm	Attributes	Applicable major release
Name: IK8451303 (6959) Type: environmentalAlarm Package: lmg.IK8451303 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: An HSV110 controller's battery assembly has been removed. The Battery Present flag for battery assembly '2' located within the HSV110 controller identified in the handle field has changed from PRESENT to NOT PRESENT indicating that the battery assembly was removed. The secondary_id field contains the battery assembly '2' internal identifier value: 2. The value.ul1 field contains the new state of the Battery Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Battery Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_1f		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1107 IK8451306

Alarm	Attributes	Applicable major release
Name: IK8451306 (6960) Type: environmentalAlarm Package: lmg.IK8451306 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: An HSV110 controller's battery assembly has malfunctioned. The Battery In Use flag for battery assembly '2' located within the HSV110 controller identified in the handle field has transitioned from the IN USE to NOT IN USE state indicating that the battery assembly has malfunctioned. The secondary_id field contains the battery assembly '2' internal identifier value: 2. The value.ul1 field contains the new state of the Battery In Use flag: 0 (NOT IN USE). The value.ul2 field contains the old state of the Battery In Use flag: 1 (IN USE).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_22		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1108 IK8451307

Alarm	Attributes	Applicable major release
Name: IK8451307 (6961) Type: equipmentAlarm Package: lmg.IK8451307 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Blower Present flag for the '2' blower assembly located within the HSV110 controller identified in the handle field has transitioned from the PRESENT to NOT PRESENT state indicating that the blower has been removed. The secondary_id field contains the '2' blower assembly internal identifier value: 2. The value.ul1 field contains the new state of the Blower Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Blower Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_23		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1109 IK8451309

Alarm	Attributes	Applicable major release
Name: IK8451309 (6962) Type: equipmentAlarm Package: lmg.IK8451309 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The '2' blower located within the HSV110 controller identified in the handle field is running slower than the lowest acceptable speed. The secondary_id field contains the '2' blower assembly internal identifier value: 2. The value.ul1 field contains the current speed of the '2' blower. The value.ul2 field contains the lowest acceptable speed for the '2' blower.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_25		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1110 IK8451310

Alarm	Attributes	Applicable major release
Name: IK8451310 (6963) Type: equipmentAlarm Package: lmg.IK8451310 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: An HSV110 controller's '1' blower/power supply assembly has been removed or AC power has been removed from the power supply. The HSV110 controller is identified in the handle field. The secondary_id field contains the '1' blower/power supply assembly internal identifier value: 1. The value.ul1 field contains the new state of the Blower/Power Supply Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Blower/Power Supply Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_26		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1111 IK8451312

Alarm	Attributes	Applicable major release
Name: IK8451312 (6964) Type: equipmentAlarm Package: lmg.IK8451312 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: An HSV110 controller's '2' blower/power supply assembly has been removed or AC power has been removed from the power supply. The HSV110 controller is identified in the handle field. The secondary_id field contains the '2' blower/power supply assembly internal identifier value: 2. The value.ul1 field contains the new state of the Blower/Power Supply Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Blower/Power Supply Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_28		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1112 IK8451314

Alarm	Attributes	Applicable major release
Name: IK8451314 (6965) Type: equipmentAlarm Package: lmg.IK8451314 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The '1' blower/power supply located within the HSV110 controller identified in the handle field is running slower than the lowest acceptable speed. The secondary_id field contains the '1' blower/power supply assembly internal identifier value: 1. The value.ul1 field contains the current speed of the '1' blower/power supply. The value.ul2 field contains the lowest acceptable speed for the '1' blower/power supply.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_2a		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1113 IK8451315

Alarm	Attributes	Applicable major release
Name: IK8451315 (6966) Type: equipmentAlarm Package: lmg.IK8451315 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The '2' blower/power supply located within the HSV110 controller identified in the handle field is running slower than the lowest acceptable speed. The secondary_id field contains the '2' blower/power supply assembly internal identifier value: 2. The value.ul1 field contains the current speed of the '2' blower/power supply. The value.ul2 field contains the lowest acceptable speed for the '2' blower/power supply.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_2b		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1114 IK8451321

Alarm	Attributes	Applicable major release
Name: IK8451321 (6967) Type: equipmentAlarm Package: lmg.IK8451321 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The state of the Physical Disk Drive identified in the handle field has transitioned to the DEGRADED state. The value.ul1 field contains the new state: 2 (DEGRADED). The value.ul2 field contains the old state. The state values that may be in the value.ul2 field are as follows: . 1 =" Normal . 3 = Failed . 4 = Not present . 5 = Single Port on Fibre . The enclosure number, bay number, and rack number where the Physical Disk Drive is located are contained in the attribute.value.u32[0], attribute.value.u32[1], attribute.value.u32[2] fields, respectively. The attribute.type field contains value 1. The rack number in the attribute.value.u32[2] field will not contain a valid value until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_31"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1115 IK8451322

Alarm	Attributes	Applicable major release
Name: IK8451322 (6968) Type: equipmentAlarm Package: lmg.IK8451322 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The state of the Physical Disk Drive identified in the handle field has transitioned to the FAILED state. The value.ul1 field contains the new state: 3 (FAILED). The value.ul2 field contains the old state. The state values that may be in the value.ul2 field are as follows: . 1 =" Normal . 2 = Degraded . 4 = Not present . 5 = Single Port on Fibre . The enclosure number, bay number, and rack number where the Physical Disk Drive is located are contained in the attribute.value.u32[0], attribute.value.u32[1], attribute.value.u32[2] fields, respectively. The attribute.type field contains value 1. The rack number in the attribute.value.u32[2] field will not contain a valid value until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_32"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1116 IK8451334

Alarm	Attributes	Applicable major release
Name: IK8451334 (6969) Type: equipmentAlarm Package: lmg.IK8451334 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Physical Disk Drive identified in the handle field has disappeared. The enclosure, bay and rack where the Physical Disk Drive is located are contained in the attribute.value.u32[0], attribute.value.u32[1] and attribute.value.u32[2] fields, respectively. The attribute.type field contains the value 1.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_3e		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1117 IK8451369

Alarm	Attributes	Applicable major release
Name: IK8451369 (6970) Type: communicationsAlarm Package: lmg.IK8451369 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The state of the internal Logical Disk associated with the Virtual Disk identified in the handle field has transitioned to the SNAPSHOT OVERCOMMIT state. The value.ul1 field contains the new state: 7 (SNAPSHOT OVERCOMMIT). The value.ul2 field contains the old state. The state values that may be found in the value.ul2 field are as follows: . 1 =" Normal . 2 = Replacement delay in progress . 3 = Redundancy lost, restore in progress . 4 = Redundancy lost, restore stalled . 5 = Failed . 6 = Creation in progress . 8 = Deletion in progress . 9 = Capacity change in progress . 10 = Inoperative due to device data lost . 11 = Capacity reservation in progress . 12 = Capacity unreservation in progress .\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_cb"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1118 IK8451376

Alarm	Attributes	Applicable major release
Name: IK8451376 (6971) Type: equipmentAlarm Package: lmg.IK8451376 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Blower Present flag for the '1' blower assembly located within the HSV110 controller identified in the handle field has transitioned from the PRESENT to NOT PRESENT state indicating that the blower has been removed. The secondary_id field contains the '1' blower assembly internal identifier value: 1. The value.ul1 field contains the new state of the Blower Present flag: 0 (NOT PRESENT). The value.ul2 field contains the old state of the Blower Present flag: 1 (PRESENT).\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_9_d2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1119 IK8451384

Alarm	Attributes	Applicable major release
Name: IK8451384 (6972) Type: processingErrorAlarm Package: lmg.IK8451384 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The specified Source Virtual Disk has transitioned to the Logging state because the alternate Storage System is not accessible or the Data Replication Group is suspended. The following fields are not valid: status, blocks, vda, port, cerp_id, side.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1120 IK8451385

Alarm	Attributes	Applicable major release
Name: IK8451385 (6973) Type: processingErrorAlarm Package: lmg.IK8451385 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The specified Source Virtual Disk has transitioned to the Logging state because the Destination Virtual Disk is not accessible. The following fields are not valid: status, blocks, vda, port, cerp_id, side.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1121 IK8451387

Alarm	Attributes	Applicable major release
Name: IK8451387 (6974) Type: processingErrorAlarm Package: lmg.IK8451387 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: A Data Replication Group has entered the Failsafe Locked state due to an inaccessible or inoperative destination. Either the Destination Virtual Disk is not accessible or a Virtual Disk in the Data Replication Group is inoperative. The following fields are not valid: status, blocks, vda, port, cerp_id, side.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_4		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1122 IK8451388

Alarm	Attributes	Applicable major release
Name: IK8451388 (6975) Type: processingErrorAlarm Package: lmg.IK8451388 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: A Data Replication Group has entered the Failsafe Locked state due to an inoperative source. Either the Source Virtual Disk is not accessible or a Virtual Disk in the Data Replication Group is inoperative. The following fields are not valid: status, blocks, vda, port, cerp_id, side.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1123 IK8451389

Alarm	Attributes	Applicable major release
Name: IK8451389 (6976) Type: processingErrorAlarm Package: Img.IK8451389 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An unrecoverable read error occurred on the specified Source Virtual Disk during the Full Copy. The Virtual Disk address specified in the vda field indicates the first block in error. The Full Copy was terminated.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1124 IK8451390

Alarm	Attributes	Applicable major release
Name: IK8451390 (6977) Type: processingErrorAlarm Package: Img.IK8451390 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: A Full Copy terminated prior to completion. A remote copy error occurred due to an inaccessible alternate Storage System. The Virtual Disk address specified in the vda field indicates the first block in error. The Full Copy will continue when the Data Replication Destination is restored.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_7		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1125 IK8451391

Alarm	Attributes	Applicable major release
Name: IK8451391 (6978) Type: processingErrorAlarm Package: Img.IK8451391 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: A Full Copy terminated prior to completion. A remote copy error occurred due to an inaccessible Destination Virtual Disk. The Virtual Disk address specified in the vda field indicates the first block in error. The Full Copy will continue when the Data Replication Destination is restored.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_c_8		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1126 IK8451400

Alarm	Attributes	Applicable major release
Name: IK8451400 (6979) Type: equipmentAlarm Package: lmg.IK8451400 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Unrecognized event reported by a Drive Enclosure Environmental Monitoring Unit. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. The event was reported by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The content of the alarm_error_code field could not be translated into a known event. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_0"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1127 IK8451401

Alarm	Attributes	Applicable major release
Name: IK8451401 (6980) Type: communicationsAlarm Package: lmg.IK8451401 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-1127 IK8451401 (continued)

Alarm	Attributes	Applicable major release
Description: A physical disk drive that is not Fibre Channel compatible or cannot operate at the link rate established by the drive enclosure I/O modules was detected. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. This problem was detected during spin up of the physical disk drive installed in the drive enclosure bay identified in the alarm_error_code.field.en field. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_1"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1128 IK8451404

Alarm	Attributes	Applicable major release
Name: IK8451404 (6981) Type: communicationsAlarm Package: lmg.IK8451404 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-1128 IK8451404 (continued)

Alarm	Attributes	Applicable major release
Description: A physical disk drive that is capable of operating at the loop link rate established by the drive enclosure I/O module was found to be running at a different rate. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The affected physical disk drive is installed in the drive enclosure bay identified in the alarm_error_code.field.en field. The Fibre Channel loop on which the problem was detected is identified by the content of the alarm_error_code.field.ec field as follows: . 4 =" loop A . 5 = loop B . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_4"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1129 IK8451406

Alarm	Attributes	Applicable major release
Name: IK8451406 (6982) Type: equipmentAlarm Package: lmg.IK8451406 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1129 IK8451406 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure power supply is improperly installed or missing. This could affect the drive enclosure air flow and cause an over temperature condition. The operational power supply will automatically shut down after a short period of time, thereby disabling the drive enclosure. This condition remains active until either the problem is corrected, or the operational power supply shuts down, whichever occurs first. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the affected power supply (1 or 2) is identified in the alarm_error_code.field.en field. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_34"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1130 IK8451407

Alarm	Attributes	Applicable major release
Name: IK8451407 (6983) Type: equipmentAlarm Package: Img.IK8451407 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A drive enclosure power supply component has failed. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the affected power supply (1 or 2) is identified in the alarm_error_code.field.en field. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_35"		

Table 27-1130 IK8451407 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1131 IK8451408

Alarm	Attributes	Applicable major release
Name: IK8451408 (6984) Type: equipmentAlarm Package: lmg.IK8451408 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A drive enclosure blower is not operating properly. This could affect the drive enclosure air flow and cause an over temperature condition. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the affected blower (1 or 2) is identified in the alarm_error_code.field.en field. The cause of the improper operation is described by the content of the alarm_error_code.field.ec field as follows: . 1 =" The blower is operating at a speed that is outside of the Drive Enclosure Environmental Monitoring Unit specified range, possibly because of a bearing problem. . 2 = The blower is operating at a speed that is significantly outside of the Drive Enclosure Environmental Monitoring Unit specified range, possibly because of a bearing problem. . 3 = The blower has stopped. NOTE: The other blower (if operational) now operates at high speed and is a single point of failure. A single blower operating at high speed can provide sufficient air flow to cool an enclosure and the elements for up to 100 hours. However, operating an enclosure at temperatures approaching an overheating threshold can damage elements and may reduce the MTBF of a specific element. Hewlett-Packard therefore recommends immediate replacement of the defective blower. . 4 = The power supply reported an internal blower error. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_ num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_ num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_47"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1132 IK8451409

Alarm	Attributes	Applicable major release
Name: IK8451409 (6985) Type: equipmentAlarm Package: lmg.IK8451409 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1132 IK8451409 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure blower is improperly installed or missing. This affects the drive enclosure air flow and can cause an over temperature condition. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the affected blower (1 or 2) is identified in the alarm_error_code.field.en field. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_4b"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1133 IK8451410

Alarm	Attributes	Applicable major release
Name: IK8451410 (6986) Type: equipmentAlarm Package: Img.IK8451410 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1133 IK8451410 (continued)

Alarm	Attributes	Applicable major release
Description: Both drive enclosure blowers are missing. This severely affects the drive enclosure air flow and can cause an over temperature condition. The operational power supply(s) will automatically shut down after a short period of time, thereby disabling the drive enclosure. This condition remains active until either the problem is corrected, or the operational power supply(s) shut down, whichever occurs first. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. Note that this event is preceded by a 'drive enclosure blower is improperly installed or missing' event that identifies the location of the first missing blower. The location of the second missing blower (1 or 2) is identified in the alarm_error_code.field.en field of this event. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_4c"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1134 IK8451412

Alarm	Attributes	Applicable major release
Name: IK8451412 (6987) Type: environmentalAlarm Package: lmg.IK8451412 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG

Table 27-1134 IK8451412 (continued)

Alarm	Attributes	Applicable major release
Description: The average temperature of two of the three temperature sensor groups (i.e., Drive Enclosure Environmental Monitoring Unit, Disk Drives, and Power Supplies) exceeds the CRITICAL level. The operational power supply(s) will automatically shut down after a short period of time, thereby disabling the drive enclosure. This condition remains active until either the problem is corrected, or the operational power supply(s) shut down, whichever occurs first. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. Note that in this case the content of the alarm_error_code.field.en field is undefined. The actual temperature threshold values can be found in the HSV element manager GUI. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_5f"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1135 IK8451419

Alarm	Attributes	Applicable major release
Name: IK8451419 (6988) Type: equipmentAlarm Package: Img.IK8451419 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1135 IK8451419 (continued)

Alarm	Attributes	Applicable major release
Description: A Drive Enclosure Environmental Monitoring Unit has experienced a hardware failure. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The alarm_error_code.field.en field contains the value 1 signifying that the Drive Enclosure Environmental Monitoring Unit is the affected element. The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 =" Loop A, 1 = Loop B) identified in the loop field. The The location of an available drive enclosure is determined by the content of the enclosures. dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release. The cause of the improper operation is described by the content of the alarm_error_code.field.ec field as follows: . 15 = Drive Enclosure Environmental Monitoring Unit hardware failure DP. . 18 = Drive Enclosure Environmental Monitoring Unit hardware failed BT. . 19 = Drive Enclosure Environmental Monitoring Unit ESI driver failure. .\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_83"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1136 IK8451421

Alarm	Attributes	Applicable major release
Name: IK8451421 (6989) Type: communicationsAlarm Package: lmg.IK8451421 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-1136 IK8451421 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure transceiver error has been detected. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the transceiver (1 through 4) is identified in the alarm_error_code.field.en field as follows: . 1 =" Transceiver 01 . 2 = Transceiver 02 . 3 = Transceiver 03 . 4 = Transceiver 04 . The transceiver error condition is described by the content of the alarm_error_code.field.ec field as follows: . 1 = The transceivers on this link are not the same type or they are incompatible with the drive enclosure I/O module. This error prevents the controller from establishing a link with the enclosure drives and eliminates the enclosure dual-loop capability. . 2 = The transceiver can no longer detect a data signal. This error prevents the controller from transferring data on a loop and eliminates the enclosure dual-loop capability. . 3 = The system has detected an FC-AL bus fault involving a transceiver. This error prevents the controller from transferring data on a loop and eliminates the enclosure dual-loop capability. . 4 = The transceiver that was previously in this location has been removed. . 5 = The transceiver in the specified location has detected invalid Fibre Channel characters. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_8d"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1137 IK8451422

Alarm	Attributes	Applicable major release
Name: IK8451422 (6990) Type: equipmentAlarm Package: Img.IK8451422 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1137 IK8451422 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure power supply voltage sensor out of range condition has been reported. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the voltage sensor (1 through 4) is identified in the alarm_error_code.field.en field as follows: . 1 =" Power Supply 1 +5 VDC . 2 = Power Supply 1 +12 VDC . 3 = Power Supply 2 +5 VDC . 4 = Power Supply 2 +12 VDC . The voltage sensor out of range condition is described by the content of the alarm_error_code.field.ec field as follows: . 1 = The element voltage is approaching, but has not reached, the high voltage CRITICAL threshold. Continued operation under these conditions may result in a CRITICAL condition. . 2 = The element voltage is above the high voltage CRITICAL threshold. . 3 = The element voltage is approaching, but has not reached, the low voltage CRITICAL threshold. Continued operation under these conditions may result in a CRITICAL condition. . 4 = The element voltage has reached the low voltage CRITICAL threshold. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_a1"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1138 IK8451423

Alarm	Attributes	Applicable major release
Name: IK8451423 (6991) Type: equipmentAlarm Package: lmg.IK8451423 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1138 IK8451423 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure power supply current sensor out of range condition has been reported. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the current sensor (1 through 4) is identified in the alarm_error_code.field.en field as follows: . 1 =" Power Supply 1 +5 VDC . 2 = Power Supply 1 +12 VDC . 3 = Power Supply 2 +5 VDC . 4 = Power Supply 2 +12 VDC . The current sensor out of range condition is described by the content of the alarm_error_code.field.ec field as follows: . 1 = The element current is approaching, but has not reached, the high current CRITICAL threshold. Continued operation under these conditions may result in a CRITICAL condition. . 2 = The element current is above the high current CRITICAL threshold. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_b5"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1139 IK8451425

Alarm	Attributes	Applicable major release
Name: IK8451425 (6992) Type: equipmentAlarm Package: lmg.IK8451425 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1139 IK8451425 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure backplane error has occurred. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The alarm_error_code. field.en field contains the value 1 signifying that the drive enclosure is the affected element. The cause of the improper operation is described by the content of the alarm_error_code.field.ec field as follows: . 11 =" Unable to write data to the NVRAM. This problem prevents communication between elements in the enclosure. . 12 = Unable to read data from the NVRAM. This problem prevents communication between elements in the enclosure. . 13 = NVRAM has not been initialized properly. This is a manufacturing error. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_ num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_ num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_d9"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1140 IK8451426

Alarm	Attributes	Applicable major release
Name: IK8451426 (6993) Type: communicationsAlarm Package: lmg.IK8451426 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-1140 IK8451426 (continued)

Alarm	Attributes	Applicable major release
Description: A drive enclosure I/O module error has occurred. The handle field contains the WWN of the drive enclosure containing the Drive Enclosure Environmental Monitoring Unit. This problem was detected by the Drive Enclosure Environmental Monitoring Unit located in the drive enclosure determined by the content of the dencl_num field as follows: . If dencl_num is less than 99, the location is as indicated by the content of the rack_num and dencl_num fields. . If dencl_num is equal to 99, the location is unknown. Note that the content of the rack_num field is undefined in this case. . If dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the rack_num and dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the rack_num field will not be valid until a future release. The location of the I/O module (A (01) and B (02)) is identified in the alarm_error_code.field.en field. The cause of the improper operation is described by the content of the alarm_error_code.field.ec field as follows: . 1 =" The I/O module's Fibre Channel link speed is not supported by the backplane. This error prevents the controller from establishing a link with enclosure drives and eliminates the enclosure dual-loop capability. . 11 = Unable to write data to the I/O module NVRAM. . 12 = Unable to read data from the I/O module NVRAM. . 13 = The I/O module that was in this location has been removed. . The enclosures array shows the drive enclosures available on the Fibre Channel loop pair (0 = Loop A, 1 = Loop B) identified in the loop field. The location of an available drive enclosure is determined by the content of the enclosures.dencl_num field as follows: . If enclosures.dencl_num is less than 99, the location is as indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. . If enclosures.dencl_num is equal to 99, the enclosures array entry is not used. Note that the content of the enclosures.rack_num field is undefined in this case. . If enclosures.dencl_num is greater than 99, the HSV110 controller does not have proof of the current location but the last known location is indicated by the content of the enclosures.rack_num and enclosures.dencl_num fields. Subtract 100 from the content of those fields to determine the actual last known location. If there have been no configuration changes, the last known location values will be accurate. . Note that the content of the enclosures.rack_num field will not be valid until a future release.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_d_dd"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1141 IK8451435

Alarm	Attributes	Applicable major release
Name: IK8451435 (6994) Type: equipmentAlarm Package: lmg.IK8451435 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A failure was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_0		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1142 IK8451437

Alarm	Attributes	Applicable major release
Name: IK8451437 (6995) Type: environmentalAlarm Package: lmg.IK8451437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG

Table 27-1142 IK8451437 (continued)

Alarm	Attributes	Applicable major release
Description: A battery assembly failure was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1143 IK8451438

Alarm	Attributes	Applicable major release
Name: IK8451438 (6996) Type: environmentalAlarm Package: lmg.IK8451438 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: A battery assembly failure was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_3		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1144 IK8451439

Alarm	Attributes	Applicable major release
Name: IK8451439 (6997) Type: communicationsAlarm Package: lmg.IK8451439 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A battery assembly communication failure was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_4		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1145 IK8451440

Alarm	Attributes	Applicable major release
Name: IK8451440 (6998) Type: communicationsAlarm Package: lmg.IK8451440 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A battery assembly communication failure was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1146 IK8451441

Alarm	Attributes	Applicable major release
Name: IK8451441 (6999) Type: processingErrorAlarm Package: lmg.IK8451441 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: StorageCell Event Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: A soft cache memory ECC error or indication of low battery voltage was detected during the execution of this HSV110 controller's on board diagnostics.\nAlarm to be cleared by the operator at the management system.\nReason: sCellEventTrap_83_6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1147 IK8452265

Alarm	Attributes	Applicable major release
Name: IK8452265 (7000) Type: environmentalAlarm Package: lmg.IK8452265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1148 IK8452272

Alarm	Attributes	Applicable major release
Name: IK8452272 (7001) Type: environmentalAlarm Package: lmg.IK8452272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1149 IK8452279

Alarm	Attributes	Applicable major release
Name: IK8452279 (7002) Type: environmentalAlarm Package: lmg.IK8452279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1150 IK8452291

Alarm	Attributes	Applicable major release
Name: IK8452291 (7003) Type: equipmentAlarm Package: lmg.IK8452291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-1151 IK8452292

Alarm	Attributes	Applicable major release
Name: IK8452292 (7004) Type: environmentalAlarm Package: lmg.IK8452292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1152 IK8452295

Alarm	Attributes	Applicable major release
Name: IK8452295 (7005) Type: equipmentAlarm Package: lmg.IK8452295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-1153 IK8452302

Alarm	Attributes	Applicable major release
Name: IK8452302 (7006) Type: equipmentAlarm Package: lmg.IK8452302 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-1154 IK8452331

Alarm	Attributes	Applicable major release
Name: IK8452331 (7007) Type: qualityOfServiceAlarm Package: lmg.IK8452331 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: BusMonRisongThresholdTrap Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: The SNMP alarm that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.\nAlarm to be cleared by the operator at the management system.\nReason: cpqn52nnBusMonRisingThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1155 IK8452332

Alarm	Attributes	Applicable major release
Name: IK8452332 (7008) Type: qualityOfServiceAlarm Package: lmg.IK8452332 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: BusMonFallingThresholdTrap Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: The SNMP alarm that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.\nAlarm to be cleared by the operator at the management system.\nReason: cpqn52nnBusMonFallingThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1156 IK8452333

Alarm	Attributes	Applicable major release
Name: IK8452333 (7009) Type: equipmentAlarm Package: lmg.IK8452333 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: GlobalBcastMemCongestionTrap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The SNMP alarm that is generated when an alarm entry crosses its rising or falling threshold and generates an event that is configured for sending SNMP traps.\nAlarm to be cleared by the operator at the management system.\nReason: cpqb52nnGlobalBcastMemCongestionTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1157 IK8452334

Alarm	Attributes	Applicable major release
Name: IK8452334 (7010) Type: equipmentAlarm Package: lmg.IK8452334 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: PortTxPktCongestionTrap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The SNMP alarm that is generated when an alarm entry crosses its rising or falling threshold and generates an event that is configured for sending SNMP traps.\nAlarm to be cleared by the operator at the management system.\nReason: cpqb52nnPortTxPktCongestionTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1158 IK8452335

Alarm	Attributes	Applicable major release
Name: IK8452335 (7011) Type: equipmentAlarm Package: lmg.IK8452335 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: PortRxMemCongestionTrap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The SNMP alarm that is generated when an alarm entry crosses its rising or falling threshold and generates an event that is configured for sending SNMP traps.\nAlarm to be cleared by the operator at the management system.\nReason: cpqb52nnPortRxMemCongestionTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1159 IK8452337

Alarm	Attributes	Applicable major release
Name: IK8452337 (7012) Type: communicationsAlarm Package: lmg.IK8452337 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1160 IK8452341

Alarm	Attributes	Applicable major release
Name: IK8452341 (7013) Type: communicationsAlarm Package: lmg.IK8452341 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1161 IK8452343

Alarm	Attributes	Applicable major release
Name: IK8452343 (7014) Type: communicationsAlarm Package: lmg.IK8452343 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1162 IK8452347

Alarm	Attributes	Applicable major release
Name: IK8452347 (7015) Type: communicationsAlarm Package: lmg.IK8452347 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1163 IK8452349

Alarm	Attributes	Applicable major release
Name: IK8452349 (7016) Type: communicationsAlarm Package: lmg.IK8452349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1164 IK8452350

Alarm	Attributes	Applicable major release
Name: IK8452350 (7017) Type: processingErrorAlarm Package: Img.IK8452350 Raised on class: Img.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: trapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-1165 IK8452360

Alarm	Attributes	Applicable major release
Name: IK8452360 (7018) Type: equipmentAlarm Package: Img.IK8452360 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-1166 IK8452363

Alarm	Attributes	Applicable major release
Name: IK8452363 (7019) Type: environmentalAlarm Package: Img.IK8452363 Raised on class: Img.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1167 IK8452368

Alarm	Attributes	Applicable major release
Name: IK8452368 (7020) Type: equipmentAlarm Package: lmg.IK8452368 Raised on class: lmg.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1168 IK8452369

Alarm	Attributes	Applicable major release
Name: IK8452369 (7021) Type: equipmentAlarm Package: lmg.IK8452369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1169 IK8452374

Alarm	Attributes	Applicable major release
Name: IK8452374 (7022) Type: equipmentAlarm Package: lmg.IK8452374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-1170 IK8452375

Alarm	Attributes	Applicable major release
Name: IK8452375 (7023) Type: equipmentAlarm Package: lmg.IK8452375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-1171 IK8452376

Alarm	Attributes	Applicable major release
Name: IK8452376 (7024) Type: equipmentAlarm Package: lmg.IK8452376 Raised on class: lmg.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-1172 IK8452377

Alarm	Attributes	Applicable major release
Name: IK8452377 (7025) Type: equipmentAlarm Package: lmg.IK8452377 Raised on class: lmg.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-1173 IK8452378

Alarm	Attributes	Applicable major release
Name: IK8452378 (7026) Type: equipmentAlarm Package: lmg.IK8452378 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-1174 IK8452379

Alarm	Attributes	Applicable major release
Name: IK8452379 (7027) Type: equipmentAlarm Package: lmg.IK8452379 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-1175 IK8452380

Alarm	Attributes	Applicable major release
Name: IK8452380 (7028) Type: equipmentAlarm Package: lmg.IK8452380 Raised on class: lmg.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-1176 IK8452382

Alarm	Attributes	Applicable major release
Name: IK8452382 (7029) Type: environmentalAlarm Package: Img.IK8452382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-1177 IK8452386

Alarm	Attributes	Applicable major release
Name: IK8452386 (7030) Type: equipmentAlarm Package: Img.IK8452386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1178 IK8452387

Alarm	Attributes	Applicable major release
Name: IK8452387 (7031) Type: equipmentAlarm Package: Img.IK8452387 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1179 IK8452388

Alarm	Attributes	Applicable major release
Name: IK8452388 (7032) Type: equipmentAlarm Package: lmg.IK8452388 Raised on class: lmg.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1180 IK8452391

Alarm	Attributes	Applicable major release
Name: IK8452391 (7033) Type: processingErrorAlarm Package: lmg.IK8452391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-1181 IK8452401

Alarm	Attributes	Applicable major release
Name: IK8452401 (7034) Type: communicationsAlarm Package: lmg.IK8452401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-1182 IK8452408

Alarm	Attributes	Applicable major release
Name: IK8452408 (7035) Type: qualityOfServiceAlarm Package: Img.IK8452408 Raised on class: Img.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1183 IK8452409

Alarm	Attributes	Applicable major release
Name: IK8452409 (7036) Type: processingErrorAlarm Package: Img.IK8452409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1184 IK8452411

Alarm	Attributes	Applicable major release
Name: IK8452411 (7037) Type: equipmentAlarm Package: Img.IK8452411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1185 IK8452428

Alarm	Attributes	Applicable major release
Name: IK8452428 (7038) Type: equipmentAlarm Package: Img.IK8452428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1185 IK8452428 (continued)

Alarm	Attributes	Applicable major release
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1186 IK8452429

Alarm	Attributes	Applicable major release
Name: IK8452429 (7039) Type: equipmentAlarm Package: lmg.IK8452429 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1187 IK8452431

Alarm	Attributes	Applicable major release
Name: IK8452431 (7040) Type: equipmentAlarm Package: lmg.IK8452431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1188 IK8452432

Alarm	Attributes	Applicable major release
Name: IK8452432 (7041) Type: equipmentAlarm Package: lmg.IK8452432 Raised on class: lmg.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1189 IK8452436

Alarm	Attributes	Applicable major release
Name: IK8452436 (7042) Type: equipmentAlarm Package: lmg.IK8452436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1190 IK8452437

Alarm	Attributes	Applicable major release
Name: IK8452437 (7043) Type: equipmentAlarm Package: lmg.IK8452437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1191 IK8452439

Alarm	Attributes	Applicable major release
Name: IK8452439 (7044) Type: communicationsAlarm Package: lmg.IK8452439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1192 IK8452462

Alarm	Attributes	Applicable major release
Name: IK8452462 (9918) Type: environmentalAlarm Package: lmg.IK8452462 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR16.1.MG

Table 27-1192 IK8452462 (continued)

Alarm	Attributes	Applicable major release
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-1193 IK8452464

Alarm	Attributes	Applicable major release
Name: IK8452464 (9919) Type: equipmentAlarm Package: Img.IK8452464 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1194 IK8452468

Alarm	Attributes	Applicable major release
Name: IK8452468 (9920) Type: equipmentAlarm Package: Img.IK8452468 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1195 IK8452494

Alarm	Attributes	Applicable major release
Name: IK8452494 (9923) Type: equipmentAlarm Package: Img.IK8452494 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutpu-tOverload		
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-1196 IK8452496

Alarm	Attributes	Applicable major release
Name: IK8452496 (9924) Type: environmentalAlarm Package: Img.IK8452496 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-1197 IK8452508

Alarm	Attributes	Applicable major release
Name: IK8452508 (9931) Type: equipmentAlarm Package: Img.IK8452508 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1198 IK8452510

Alarm	Attributes	Applicable major release
Name: IK8452510 (9932) Type: environmentalAlarm Package: Img.IK8452510 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-1199 IK8452518

Alarm	Attributes	Applicable major release
Name: IK8452518 (9935) Type: equipmentAlarm Package: lmg.IK8452518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1200 IK8452531

Alarm	Attributes	Applicable major release
Name: IK8452531 (9940) Type: equipmentAlarm Package: lmg.IK8452531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-1201 IK8452533

Alarm	Attributes	Applicable major release
Name: IK8452533 (9941) Type: equipmentAlarm Package: lmg.IK8452533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInputOutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-1202 IK8452534

Alarm	Attributes	Applicable major release
Name: IK8452534 (9942) Type: environmentalAlarm Package: lmg.IK8452534 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTemperatureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-1203 IK8452536

Alarm	Attributes	Applicable major release
Name: IK8452536 (9943) Type: equipmentAlarm Package: lmg.IK8452536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassOnAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-1204 IK8452539

Alarm	Attributes	Applicable major release
Name: IK8452539 (9945) Type: equipmentAlarm Package: lmg.IK8452539 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-1205 IK8452541

Alarm	Attributes	Applicable major release
Name: IK8452541 (9946) Type: environmentalAlarm Package: lmg.IK8452541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-1206 IK8452543

Alarm	Attributes	Applicable major release
Name: IK8452543 (9947) Type: equipmentAlarm Package: lmg.IK8452543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1207 IK8452546

Alarm	Attributes	Applicable major release
Name: IK8452546 (9949) Type: equipmentAlarm Package: lmg.IK8452546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1208 IK8452548

Alarm	Attributes	Applicable major release
Name: IK8452548 (9950) Type: environmentalAlarm Package: Img.IK8452548 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1209 IK8452550

Alarm	Attributes	Applicable major release
Name: IK8452550 (9951) Type: environmentalAlarm Package: Img.IK8452550 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If the problem persists, contact NOKIA customer support.		

Table 27-1210 IK8452552

Alarm	Attributes	Applicable major release
Name: IK8452552 (9952) Type: processingErrorAlarm Package: Img.IK8452552 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-1211 IK8452554

Alarm	Attributes	Applicable major release
Name: IK8452554 (9953) Type: equipmentAlarm Package: lmg.IK8452554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-1212 IK8452556

Alarm	Attributes	Applicable major release
Name: IK8452556 (9954) Type: equipmentAlarm Package: lmg.IK8452556 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-1213 IK8452559

Alarm	Attributes	Applicable major release
Name: IK8452559 (7045) Type: equipmentAlarm Package: lmg.IK8452559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-1214 IK8452609

Alarm	Attributes	Applicable major release
Name: IK8452609 (7046) Type: processingErrorAlarm Package: Img.IK8452609 Raised on class: Img.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1215 IK8452610

Alarm	Attributes	Applicable major release
Name: IK8452610 (7047) Type: processingErrorAlarm Package: Img.IK8452610 Raised on class: Img.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1216 IK8452615

Alarm	Attributes	Applicable major release
Name: IK8452615 (7048) Type: equipmentAlarm Package: Img.IK8452615 Raised on class: Img.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-1217 IK8452616

Alarm	Attributes	Applicable major release
Name: IK8452616 (7049) Type: environmentalAlarm Package: lmg.IK8452616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-1218 IK8452617

Alarm	Attributes	Applicable major release
Name: IK8452617 (7050) Type: environmentalAlarm Package: lmg.IK8452617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-1219 IK8452620

Alarm	Attributes	Applicable major release
Name: IK8452620 (7051) Type: equipmentAlarm Package: lmg.IK8452620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-1220 IK8452622

Alarm	Attributes	Applicable major release
Name: IK8452622 (7052) Type: environmentalAlarm Package: Img.IK8452622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-1221 IK8452628

Alarm	Attributes	Applicable major release
Name: IK8452628 (7053) Type: equipmentAlarm Package: Img.IK8452628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-1222 IK8452632

Alarm	Attributes	Applicable major release
Name: IK8452632 (7054) Type: processingErrorAlarm Package: Img.IK8452632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1223 IK8452633

Alarm	Attributes	Applicable major release
Name: IK8452633 (7055) Type: communicationsAlarm Package: lmg.IK8452633 Raised on class: lmg.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-1224 IK8452636

Alarm	Attributes	Applicable major release
Name: IK8452636 (9250) Type: equipmentAlarm Package: lmg.IK8452636 Raised on class: lmg.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1225 IK8452648

Alarm	Attributes	Applicable major release
Name: IK8452648 (7056) Type: qualityOfServiceAlarm Package: lmg.IK8452648 Raised on class: lmg.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1226 IK8452657

Alarm	Attributes	Applicable major release
Name: IK8452657 (7057) Type: environmentalAlarm Package: lmg.IK8452657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1227 IK8452707

Alarm	Attributes	Applicable major release
Name: IK8452707 (7058) Type: environmentalAlarm Package: lmg.IK8452707 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: UPS Battery Low Implicitly cleared: false Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG
Description: UPS Battery Low. The server will soon lose power.\nAlarm to be cleared by the operator at the management system.\nReason: cpqUpsBatteryLow		
Remedial action: Check the UPS Battery		

Table 27-1228 IK8452708

Alarm	Attributes	Applicable major release
Name: IK8452708 (9251) Type: equipmentAlarm Package: lmg.IK8452708 Raised on class: lmg.FRU	Severity: major Specific problem: AC Line Failure Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: AC Line power failure. The UPS reports that the AC line power has failed.\nAlarm is cleared by the system.\nReason: cpqUps2LineFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1229 IK8452712

Alarm	Attributes	Applicable major release
Name: IK8452712 (7059) Type: environmentalAlarm Package: lmg.IK8452712 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: UPS Battery Low Implicitly cleared: false Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG

Table 27-1229 IK8452712 (continued)

Alarm	Attributes	Applicable major release
Description: UPS Battery Low. The server will soon lose power.\nAlarm to be cleared by the operator at the management system.\nReason: cpqUps2BatteryLow		
Remedial action: Check the UPS Battery		

Table 27-1230 IK8452714

Alarm	Attributes	Applicable major release
Name: IK8452714 (7060) Type: environmentalAlarm Package: lmg.IK8452714 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: UPS Pending Battery Failure Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: The UPS battery is about to fail. Replace as soon as possible.\nAlarm to be cleared by the operator at the management system.\nReason: cpqUpsPendingBatteryFailure		
Remedial action: Replace the failing UPS batery		

Table 27-1231 IK8452715

Alarm	Attributes	Applicable major release
Name: IK8452715 (7061) Type: equipmentAlarm Package: lmg.IK8452715 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: UPS Critical Alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Generic UPS critical alarm.\nAlarm to be cleared by the operator at the management system.\nReason: cpqUpsGeneric-Critical		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1232 IK8452919

Alarm	Attributes	Applicable major release
Name: IK8452919 (9252) Type: communicationsAlarm Package: lmg.IK8452919 Raised on class: lmg.FRU	Severity: major Specific problem: bntSwDefGwDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSwDefGwDown alarm signifies that the default gateway is down.\nAlarm is cleared by the system.\nReason: bntSwDefGwDown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1233 IK8452921

Alarm	Attributes	Applicable major release
Name: IK8452921 (9253) Type: equipmentAlarm Package: Img.IK8452921 Raised on class: Img.FRU	Severity: major Specific problem: bntSwDefGwNotInService Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSwDefGwDisabled alarm signifies that the default gateway is alive but not in service.\nAlarm is cleared by the system.\nReason: bntSwDefGwNotInService		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1234 IK8452927

Alarm	Attributes	Applicable major release
Name: IK8452927 (9254) Type: processingErrorAlarm Package: Img.IK8452927 Raised on class: Img.FRU	Severity: major Specific problem: bntSwFwDownloadFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSwFwDownloadFailure signifies that firmware downloaded failed to [image1|image2|boot image].\nAlarm is cleared by the system.\nReason: bntSwFwDownloadFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1235 IK8452929

Alarm	Attributes	Applicable major release
Name: IK8452929 (9255) Type: communicationsAlarm Package: Img.IK8452929 Raised on class: Img.FRU	Severity: major Specific problem: bntSwUfdfoLtMFailure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSwUfdfoLtMFailure alarm signifies that a LtM link is down.\nAlarm is cleared by the system.\nReason: bntSwUfdfoLtMFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1236 IK8452932

Alarm	Attributes	Applicable major release
Name: IK8452932 (9256) Type: equipmentAlarm Package: Img.IK8452932 Raised on class: Img.FRU	Severity: major Specific problem: bntSwUfdfoGlobalDis Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG

Table 27-1236 IK8452932 (continued)

Alarm	Attributes	Applicable major release
Description: A bntSwUfdfoGlobalDis alarm signifies that Global UFD is disabled.\nAlarm is cleared by the system.\nReason: bntSwUfdfoGlobalDis		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1237 IK8452934

Alarm	Attributes	Applicable major release
Name: IK8452934 (9257) Type: communicationsAlarm Package: lmg.IK8452934 Raised on class: lmg.FRU	Severity: major Specific problem: bntSwUfdfoLtDAutoDis Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSwUfdfoLtDAutoDis alarm signifies that a LtD link is Auto Disabled.\nAlarm is cleared by the system.\nReason: bntSwUfdfoLtDAutoDis		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1238 IK8452940

Alarm	Attributes	Applicable major release
Name: IK8452940 (9258) Type: equipmentAlarm Package: lmg.IK8452940 Raised on class: lmg.FRU	Severity: major Specific problem: A bntSFPRemoved trap signifies that a SFP is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A bntSFPRemoved alarm signifies that a SFP is removed.\nAlarm is cleared by the system.\nReason: bntSFPRemoved		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1239 IK8452986

Alarm	Attributes	Applicable major release
Name: IK8452986 (7062) Type: environmentalAlarm Package: lmg.IK8452986 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: hpTempHighCritical753 Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: One of the temperature sensors crossed its upper critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hpTempHighCritical753		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1240 IK8452989

Alarm	Attributes	Applicable major release
Name: IK8452989 (7063) Type: environmentalAlarm Package: lmg.IK8452989 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Temperature Emergency Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: One of the temperature sensors crossed its upper critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPTemperature5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1241 IK8452992

Alarm	Attributes	Applicable major release
Name: IK8452992 (7064) Type: environmentalAlarm Package: lmg.IK8452992 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: hpTemperature756 Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: One of the temperature sensors crossed its upper critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hpTemperature756		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1242 IK8452998

Alarm	Attributes	Applicable major release
Name: IK8452998 (7065) Type: equipmentAlarm Package: lmg.IK8452998 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Voltage reached critical level Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage degraded to critical level from less severe -\nAlarm to be cleared by the operator at the management system.\nReason: hpEnvironment728		
Remedial action: Check all boards with this voltage		

Table 27-1243 IK8453000

Alarm	Attributes	Applicable major release
Name: IK8453000 (7066) Type: equipmentAlarm Package: lmg.IK8453000 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Power Pod Voltage Fault Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1243 IK8453000 (continued)

Alarm	Attributes	Applicable major release
Description: Voltage becomes non-recoverable from either critical level or less severe level -\nAlarm to be cleared by the operator at the management system.\nReason: hpEnvironment706		
Remedial action: Check all boards with this voltage		

Table 27-1244 IK8453025

Alarm	Attributes	Applicable major release
Name: IK8453025 (7067) Type: equipmentAlarm Package: lmg.IK8453025 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: time critical shutdown Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: OS run-time critical shutdown\nAlarm to be cleared by the operator at the management system.\nReason: hpSystemHW748		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1245 IK8454220

Alarm	Attributes	Applicable major release
Name: IK8454220 (7068) Type: processingErrorAlarm Package: lmg.IK8454220 Raised on class: lmg.FRU	Severity: critical Specific problem: N The device's health has changed to critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: N The device's health has changed to critical.\nAlarm is cleared by the system.\nReason: hpHttpMgCriticalHealthTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1246 IK8454221

Alarm	Attributes	Applicable major release
Name: IK8454221 (7069) Type: processingErrorAlarm Package: lmg.IK8454221 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Recoverable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: N The device's health has changed to Non-Recoverable.\nAlarm to be cleared by the operator at the management system.\nReason: hpHttpMgNonRecoverableHealthTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1247 IK8454239

Alarm	Attributes	Applicable major release
Name: IK8454239 (9259) Type: equipmentAlarm Package: Img.IK8454239 Raised on class: Img.FRU	Severity: major Specific problem: hpmcSGSubnetDown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Sent when ServiceGuard detects that a previously operational subnet is now down.\nAlarm is cleared by the system.\nReason: hpmcSGSubnetDown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1248 IK8454246

Alarm	Attributes	Applicable major release
Name: IK8454246 (9260) Type: equipmentAlarm Package: Img.IK8454246 Raised on class: Img.FRU	Severity: major Specific problem: hpmcSGSubnet6Down Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Sent when ServiceGuard detects that a previously operational IPv6 subnet is now down.\nAlarm is cleared by the system.\nReason: hpmcSGSubnet6Down		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1249 IK8454295

Alarm	Attributes	Applicable major release
Name: IK8454295 (9955) Type: communicationsAlarm Package: Img.IK8454295 Raised on class: Img.FRU	Severity: indeterminate Specific problem: hpSwitch516733-B21trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A general event log for 516733-B21 HP Networking E6120-XG Switch.\nReason: hpSwitch516733_B21trap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1250 IK8454370

Alarm	Attributes	Applicable major release
Name: IK8454370 (7070) Type: processingErrorAlarm Package: Img.IK8454370 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Corrupt Devices File Implicitly cleared: false Default probable cause: corruptData	Release: • LR14.3.MG

Table 27-1250 IK8454370 (continued)

Alarm	Attributes	Applicable major release
Description: Device Database has been corrupted.\nAlarm to be cleared by the operator at the management system.\nReason: adaptecSCSI1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1251 IK8454371

Alarm	Attributes	Applicable major release
Name: IK8454371 (7071) Type: processingErrorAlarm Package: lmg.IK8454371 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Corrupt Devices File Implicitly cleared: false Default probable cause: corruptData	Release: • LR14.3.MG
Description: Device Database has been corrupted.\nAlarm to be cleared by the operator at the management system.\nReason: adaptecSCSI2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1252 IK8454418

Alarm	Attributes	Applicable major release
Name: IK8454418 (7072) Type: equipmentAlarm Package: lmg.IK8454418 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: HPDA Logical Drive: Critical Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: HPDA Logical Drive: Critical\nAlarm to be cleared by the operator at the management system.\nReason: hPRaid3		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1253 IK8454423

Alarm	Attributes	Applicable major release
Name: IK8454423 (7073) Type: equipmentAlarm Package: lmg.IK8454423 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: HPDA Hard Disk Failed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: HPDA Hard Disk Failed\nAlarm to be cleared by the operator at the management system.\nReason: hPRaid8		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1254 IK8454424

Alarm	Attributes	Applicable major release
Name: IK8454424 (7074) Type: equipmentAlarm Package: Img.IK8454424 Raised on class: Img.LMGMngElement	Severity: major Specific problem: HPDA Hard Disk Failed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: HPDA Hard Disk Failed\nAlarm to be cleared by the operator at the management system.\nReason: hPRaid9		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1255 IK8454429

Alarm	Attributes	Applicable major release
Name: IK8454429 (7075) Type: equipmentAlarm Package: Img.IK8454429 Raised on class: Img.LMGMngElement	Severity: major Specific problem: HPDA Threshold Exceeded: Hardware Errors Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: HPDA Threshold Exceeded: Hardware Errors\nAlarm to be cleared by the operator at the management system.\nReason: hPRaid14		
Remedial action: check HPDA		

Table 27-1256 IK8454430

Alarm	Attributes	Applicable major release
Name: IK8454430 (7076) Type: equipmentAlarm Package: Img.IK8454430 Raised on class: Img.LMGMngElement	Severity: major Specific problem: HPDA Threshold Exceeded: Hardware Errors Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: HPDA Threshold Exceeded: Hardware Errors\nAlarm to be cleared by the operator at the management system.\nReason: hPRaid15		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1257 IK8454441

Alarm	Attributes	Applicable major release
Name: IK8454441 (7077) Type: equipmentAlarm Package: Img.IK8454441 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Voltage Warning Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1257 IK8454441 (continued)

Alarm	Attributes	Applicable major release
Description: One of the voltage sensors crossed its upper non-critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPEnvironment4		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1258 IK8454442

Alarm	Attributes	Applicable major release
Name: IK8454442 (7078) Type: equipmentAlarm Package: lmg.IK8454442 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Voltage Emergency Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One of the voltage sensors crossed its upper critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPEnvironment5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1259 IK8454443

Alarm	Attributes	Applicable major release
Name: IK8454443 (7079) Type: equipmentAlarm Package: lmg.IK8454443 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Voltage Emergency Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One of the voltage sensors crossed its upper non-recoverable threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPEnvironment6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1260 IK8454444

Alarm	Attributes	Applicable major release
Name: IK8454444 (7080) Type: equipmentAlarm Package: lmg.IK8454444 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Voltage Regulating Module Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage Regulating Module (VRM) on the indicated processor module had failed.\nAlarm to be cleared by the operator at the management system.\nReason: hPEnvironment7		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1261 IK8454449

Alarm	Attributes	Applicable major release
Name: IK8454449 (7081) Type: environmentalAlarm Package: lmg.IK8454449 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Fan Emergency Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: One of the fan sensors crossed its upper critical threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPFan5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1262 IK8454450

Alarm	Attributes	Applicable major release
Name: IK8454450 (7082) Type: environmentalAlarm Package: lmg.IK8454450 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Fan Emergency Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: One of the fan sensors crossed its upper non-recoverable threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hPFan6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1263 IK8454452

Alarm	Attributes	Applicable major release
Name: IK8454452 (7083) Type: environmentalAlarm Package: lmg.IK8454452 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Processor/PCI Fan Tray failure Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: Two or more of the fans in the Processor/PCI Fan Tray have stopped or have been removed.\nAlarm to be cleared by the operator at the management system.\nReason: hPFan8		
Remedial action: Check the fans in the Processor/PCI Fan Tray		

Table 27-1264 IK8454454

Alarm	Attributes	Applicable major release
Name: IK8454454 (7084) Type: environmentalAlarm Package: lmg.IK8454454 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Memory Fan Error Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG

Table 27-1264 IK8454454 (continued)

Alarm	Attributes	Applicable major release
Description: One of the fans in the Memory Fan Tray stopped.\nAlarm to be cleared by the operator at the management system.\nReason: hPFan10		
Remedial action: check the fans in the Memory Fan Tray		

Table 27-1265 IK8454455

Alarm	Attributes	Applicable major release
Name: IK8454455 (7085) Type: environmentalAlarm Package: lmg.IK8454455 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Memory Fan Failure Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: Two or more of the fans in the Memory Fan Tray have stopped or been removed.\nAlarm to be cleared by the operator at the management system.\nReason: hPFan11		
Remedial action: Check the fans in the Memory Fan Tray		

Table 27-1266 IK8454481

Alarm	Attributes	Applicable major release
Name: IK8454481 (7086) Type: processingErrorAlarm Package: lmg.IK8454481 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Alignment Errors exceeded threshold Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The total number of alignment and CRC errors has exceeded the threshold.\nAlarm to be cleared by the operator at the management system.\nReason: networkCard13		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1267 IK8454541

Alarm	Attributes	Applicable major release
Name: IK8454541 (7087) Type: equipmentAlarm Package: lmg.IK8454541 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Warning NOS hang Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: ASR has stopped notifying the HP Remote Assistant Card that the system is running correctly (the server probably hung or crashed).\nAlarm to be cleared by the operator at the management system.\nReason: rAASR1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1268 IK8454560

Alarm	Attributes	Applicable major release
Name: IK8454560 (7088) Type: equipmentAlarm Package: Img.IK8454560 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Automatic power shutdown due to critical condition Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Automatic power shutdown due to critical condition.\nAlarm to be cleared by the operator at the management system.\nReason: rAOther15		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1269 IK8454591

Alarm	Attributes	Applicable major release
Name: IK8454591 (7089) Type: equipmentAlarm Package: Img.IK8454591 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Control Card battery low Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The TopTools Remote Control backup battery has discharged to a level where it will not be able to power the card\nAlarm to be cleared by the operator at the management system.\nReason: rAOther46		
Remedial action: check the TopTools Remote Control backup battery		

Table 27-1270 IK8454595

Alarm	Attributes	Applicable major release
Name: IK8454595 (7090) Type: environmentalAlarm Package: Img.IK8454595 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Temperature Graceful Shutdown Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The server temperature measured on the HP Remote Assistant Card has exceeded the configured threshold and the server has been automatically shut down.\nAlarm to be cleared by the operator at the management system.\nReason: rATemp2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1271 IK8454596

Alarm	Attributes	Applicable major release
Name: IK8454596 (7091) Type: environmentalAlarm Package: Img.IK8454596 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Automatic graceful shutdown of NOS Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG

Table 27-1271 IK8454596 (continued)

Alarm	Attributes	Applicable major release
Description: The server temperature or voltage levels measured by the remote management hardware has exceeded the configured threshold. The server has been automatically shut down.\nAlarm to be cleared by the operator at the management system.\nReason: rATemp3		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1272 IK8454597

Alarm	Attributes	Applicable major release
Name: IK8454597 (7092) Type: environmentalAlarm Package: lmg.IK8454597 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Temperature Critical Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The server temperature measured on the HP Remote Assistant Card has exceeded the configured Graceful Shutdown threshold value by 5 degrees C and the server has been automatically shut down.\nAlarm to be cleared by the operator at the management system.\nReason: rATemp4		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1273 IK8454598

Alarm	Attributes	Applicable major release
Name: IK8454598 (7093) Type: equipmentAlarm Package: lmg.IK8454598 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Server power failure Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The server has lost the power completely.\nAlarm to be cleared by the operator at the management system.\nReason: rAVoltage1		
Remedial action: check the server power		

Table 27-1274 IK8454599

Alarm	Attributes	Applicable major release
Name: IK8454599 (7094) Type: equipmentAlarm Package: lmg.IK8454599 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: 12V Upper Threshold upper threshold warning Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage measured in the server has gone outside of -12V Upper Threshold.\nAlarm to be cleared by the operator at the management system.\nReason: rAVoltage2		

Table 27-1274 IK8454599 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1275 IK8454600

Alarm	Attributes	Applicable major release
Name: IK8454600 (7095) Type: equipmentAlarm Package: lmg.IK8454600 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: +33 Upper Threshold Warning Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage measured in the server has gone outside of +3.3V Upper Threshold.\nAlarm to be cleared by the operator at the management system.\nReason: rAVoltage3		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1276 IK8454601

Alarm	Attributes	Applicable major release
Name: IK8454601 (7096) Type: equipmentAlarm Package: lmg.IK8454601 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: +5V Upper Threshold Warning Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage measured in the server has gone outside of +5V Upper Threshold.\nAlarm to be cleared by the operator at the management system.\nReason: rAVoltage4		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1277 IK8454602

Alarm	Attributes	Applicable major release
Name: IK8454602 (7097) Type: equipmentAlarm Package: lmg.IK8454602 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: +12V Upper Threshold Warning Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage measured in the server has gone outside of +12V Upper Threshold.\nAlarm to be cleared by the operator at the management system.\nReason: rAVoltage5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1278 IK8454621

Alarm	Attributes	Applicable major release
Name: IK8454621 (7098) Type: equipmentAlarm Package: Img.IK8454621 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power System failure A/C Lost Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Power System failure A/C Lost\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower14		
Remedial action: Check Power system AC		

Table 27-1279 IK8454623

Alarm	Attributes	Applicable major release
Name: IK8454623 (7099) Type: environmentalAlarm Package: Img.IK8454623 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Over Temperature Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: Temperature alert on designated Power Supply.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower16		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1280 IK8454624

Alarm	Attributes	Applicable major release
Name: IK8454624 (7100) Type: environmentalAlarm Package: Img.IK8454624 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Over Temperature Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: Temperature alert on designated Power Supply.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower17		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1281 IK8454625

Alarm	Attributes	Applicable major release
Name: IK8454625 (7101) Type: equipmentAlarm Package: Img.IK8454625 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Fan Failed Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1281 IK8454625 (continued)

Alarm	Attributes	Applicable major release
Description: Fan failure on designated Power Supply.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower18		
Remedial action: Check the fan of the Power Supply		

Table 27-1282 IK8454626

Alarm	Attributes	Applicable major release
Name: IK8454626 (7102) Type: equipmentAlarm Package: lmg.IK8454626 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Fan Failed Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Fan failure on designated Power Supply.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower19		
Remedial action: Check the fan of the Power Supply		

Table 27-1283 IK8454630

Alarm	Attributes	Applicable major release
Name: IK8454630 (7103) Type: equipmentAlarm Package: lmg.IK8454630 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply 33 volts bad Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A power supply's 3.3 volt supply has gone bad\nAlarm to be cleared by the operator at the management system.\ nReason: redundantPower23		
Remedial action: check the 3.3V power supply		

Table 27-1284 IK8454631

Alarm	Attributes	Applicable major release
Name: IK8454631 (7104) Type: equipmentAlarm Package: lmg.IK8454631 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply 5 volts bad Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A power supply's 5 volt supply has gone bad\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower24		
Remedial action: check the 5V power supply		

Table 27-1285 IK8454632

Alarm	Attributes	Applicable major release
Name: IK8454632 (7105) Type: equipmentAlarm Package: Img.IK8454632 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply 12 volts bad Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A power supply's 12 volt supply has gone bad\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower25		
Remedial action: check the 12V power supply		

Table 27-1286 IK8454633

Alarm	Attributes	Applicable major release
Name: IK8454633 (7106) Type: equipmentAlarm Package: Img.IK8454633 Raised on class: Img.LMGMngElement	Severity: major Specific problem: 12 volts bad Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A power supply's -12 volt supply has gone bad\nAlarm to be cleared by the operator at the management system.\ nReason: redundantPower26		
Remedial action: check the -12V power supply		

Table 27-1287 IK8454634

Alarm	Attributes	Applicable major release
Name: IK8454634 (7107) Type: equipmentAlarm Package: Img.IK8454634 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Removed Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Indicated Power Supply has been removed or is not connected properly.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower27		
Remedial action: check the Power Supply		

Table 27-1288 IK8454638

Alarm	Attributes	Applicable major release
Name: IK8454638 (7108) Type: equipmentAlarm Package: Img.IK8454638 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Unit power has failed Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1288 IK8454638 (continued)

Alarm	Attributes	Applicable major release
Description: The indicated Power Supply Unit power has failed.\nAlarm to be cleared by the operator at the management system.\nReason: redundantPower31		
Remedial action: check the indicated Power Supply Unit power		

Table 27-1289 IK8454650

Alarm	Attributes	Applicable major release
Name: IK8454650 (7109) Type: processingErrorAlarm Package: lmg.IK8454650 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Capacity major level Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: Volume Storage Capacity has exceeded the major threshold level.\nAlarm to be cleared by the operator at the management system.\nReason: storageCap5		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1290 IK8454651

Alarm	Attributes	Applicable major release
Name: IK8454651 (7110) Type: processingErrorAlarm Package: lmg.IK8454651 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Capacity major level Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: Volume Storage Capacity has exceeded the major threshold level.\nAlarm to be cleared by the operator at the management system.\nReason: storageCap6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1291 IK8454659

Alarm	Attributes	Applicable major release
Name: IK8454659 (7111) Type: equipmentAlarm Package: lmg.IK8454659 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: VRM failure Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: VRM failure\nAlarm to be cleared by the operator at the management system.\nReason: systemHW7s		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1292 IK8454680

Alarm	Attributes	Applicable major release
Name: IK8454680 (7112) Type: equipmentAlarm Package: Img.IK8454680 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Processor startup/initialization failed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Processor startup/initialization failed\nAlarm to be cleared by the operator at the management system.\nReason: systemHW26		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1293 IK8454681

Alarm	Attributes	Applicable major release
Name: IK8454681 (7113) Type: equipmentAlarm Package: Img.IK8454681 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Fan failure Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Multiple Fan Failure\nAlarm to be cleared by the operator at the management system.\nReason: systemHW27		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1294 IK8454698

Alarm	Attributes	Applicable major release
Name: IK8454698 (7114) Type: equipmentAlarm Package: Img.IK8454698 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: System critical limit exceeded Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: An event of critical severity has occurred in the system. For example, both system fans have failed\nAlarm to be cleared by the operator at the management system.\nReason: systemHW44		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1295 IK8454708

Alarm	Attributes	Applicable major release
Name: IK8454708 (7115) Type: equipmentAlarm Package: Img.IK8454708 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Control Board System reset Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1295 IK8454708 (continued)

Alarm	Attributes	Applicable major release
Description: The system has been reset because Control Board detected a critical error.\nAlarm to be cleared by the operator at the management system.\nReason: systemHW54		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1296 IK8454710

Alarm	Attributes	Applicable major release
Name: IK8454710 (7116) Type: equipmentAlarm Package: Img.IK8454710 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Processor Card Missing or not terminated Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The Processor Card is missing or not properly terminated in indicated processor module.\nAlarm to be cleared by the operator at the management system.\nReason: systemHW56		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1297 IK8454712

Alarm	Attributes	Applicable major release
Name: IK8454712 (7117) Type: equipmentAlarm Package: Img.IK8454712 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Violation Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Front Panel Button Violation\nAlarm to be cleared by the operator at the management system.\nReason: systemHW58		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1298 IK8454730

Alarm	Attributes	Applicable major release
Name: IK8454730 (7118) Type: equipmentAlarm Package: Img.IK8454730 Raised on class: Img.LMGMngElement	Severity: major Specific problem: ACPI hardware failure Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: ACPI hardware failure\nAlarm to be cleared by the operator at the management system.\nReason: systemHW77		
Remedial action: check ACPI		

Table 27-1299 IK8454735

Alarm	Attributes	Applicable major release
Name: IK8454735 (7119) Type: environmentalAlarm Package: lmg.IK8454735 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The battery cycles have gone beyond the upper critical range Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Battery cycles have gone beyond the upper critical range\nAlarm to be cleared by the operator at the management system.\nReason: systemHW81		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1300 IK8454743

Alarm	Attributes	Applicable major release
Name: IK8454743 (7120) Type: processingErrorAlarm Package: lmg.IK8454743 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic trap for Critical or Fatal type E0 event from system firmware Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Generic alarm for Critical or Fatal type E0 event from system firmware\nAlarm to be cleared by the operator at the management system.\nReason: systemFW1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1301 IK8454749

Alarm	Attributes	Applicable major release
Name: IK8454749 (7121) Type: environmentalAlarm Package: lmg.IK8454749 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Temperature Emergency Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: Server temperature has exceeded the emergency temperature threshold.\nAlarm to be cleared by the operator at the management system.\nReason: temperature3		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1302 IK8454752

Alarm	Attributes	Applicable major release
Name: IK8454752 (7122) Type: environmentalAlarm Package: Img.IK8454752 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Hot Swap: Temperature emergency Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: Hot Swap Cage : Emergency temperature exceeded!\nAlarm to be cleared by the operator at the management system.\nReason: temperature6		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1303 IK8454755

Alarm	Attributes	Applicable major release
Name: IK8454755 (7123) Type: environmentalAlarm Package: Img.IK8454755 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Hot Swap Cage: Temperature emergency Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: Hot Swap Cage : Emergency temperature exceeded!\nAlarm to be cleared by the operator at the management system.\nReason: temperature9		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1304 IK8454762

Alarm	Attributes	Applicable major release
Name: IK8454762 (7124) Type: communicationsAlarm Package: Img.IK8454762 Raised on class: Img.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1305 IK8456033

Alarm	Attributes	Applicable major release
Name: IK8456033 (7125) Type: equipmentAlarm Package: lmg.IK8456033 Raised on class: lmg.FRU	Severity: major Specific problem: hpOVISMajorAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Major alarm\nAlarm is cleared by the system.\nReason: hpOVISMajorAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1306 IK8456034

Alarm	Attributes	Applicable major release
Name: IK8456034 (7126) Type: equipmentAlarm Package: lmg.IK8456034 Raised on class: lmg.FRU	Severity: critical Specific problem: hpOVISCriticalAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Critical alarm\nAlarm is cleared by the system.\nReason: hpOVISCriticalAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1307 IK8457327

Alarm	Attributes	Applicable major release
Name: IK8457327 (7127) Type: environmentalAlarm Package: lmg.IK8457327 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: hh3cEntityExtTemperatureThresholdNotification Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The hh3cEntityExtTemperatureThresholdNotification indicates the temperature exceeded the threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hh3cEntityExtTemperatureThresholdNotification		
Remedial action: Check the status and the environment of the entity, sometimes it happens because of the failure of air-condition.		

Table 27-1308 IK8457329

Alarm	Attributes	Applicable major release
Name: IK8457329 (7128) Type: equipmentAlarm Package: lmg.IK8457329 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: hh3cEntityExtVoltageHighThresholdNotification Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-1308 IK8457329 (continued)

Alarm	Attributes	Applicable major release
Description: The hh3cEntityExtVoltageHighThresholdNotification indicates the voltage is higher than the threshold. If the voltage is higher too much than the entity needs, The entity may be damaged by the high voltage.\nAlarm to be cleared by the operator at the management system.\nReason: hh3cEntityExtVoltageHighThresholdNotification		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1309 IK8457330

Alarm	Attributes	Applicable major release
Name: IK8457330 (9261) Type: equipmentAlarm Package: lmg.IK8457330 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExtCpuUsageThresholdNotfication Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The hh3cEntityExtCpuUsageThresholdNotfication indicates the entity is overloaded.\nAlarm is cleared by the system.\nReason: hh3cEntityExtCpuUsageThresholdNotfication		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1310 IK8457331

Alarm	Attributes	Applicable major release
Name: IK8457331 (7129) Type: processingErrorAlarm Package: lmg.IK8457331 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExtMemUsageThresholdNotification Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The hh3cEntityExtMemUsageThresholdNotification indicates the entity is overloaded.\nAlarm is cleared by the system.\nReason: hh3cEntityExtMemUsageThresholdNotification		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1311 IK8457333

Alarm	Attributes	Applicable major release
Name: IK8457333 (9262) Type: equipmentAlarm Package: lmg.IK8457333 Raised on class: lmg.FRU	Severity: major Specific problem: The trap indicates the entity is not operable at present Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm indicates the entity is not operable at present.\nAlarm is cleared by the system.\nReason: hh3cEntityExtOperDisabled		

Table 27-1311 IK8457333 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1312 IK8457334

Alarm	Attributes	Applicable major release
Name: IK8457334 (7130) Type: environmentalAlarm Package: lmg.IK8457334 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: hh3cEntityExtCriticalTemperatureThresholdNotification Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: The hh3cEntityExtCriticalTemperatureThresholdNotification indicates the temperature exceeds the critical temperature.\nAlarm to be cleared by the operator at the management system.\nReason: hh3cEntityExtCriticalTemperatureThresholdNotification		
Remedial action: Check the status and the environment of the entity, sometimes it happens because of the failure of air-condition.		

Table 27-1313 IK8457335

Alarm	Attributes	Applicable major release
Name: IK8457335 (9263) Type: equipmentAlarm Package: lmg.IK8457335 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExtSFPAlarmOn Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm is generated when the SFP module fails or runs abnormally for some particular reason.\nAlarm is cleared by the system.\nReason: hh3cEntityExtSFPAlarmOn		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1314 IK8457340

Alarm	Attributes	Applicable major release
Name: IK8457340 (9264) Type: equipmentAlarm Package: lmg.IK8457340 Raised on class: lmg.FRU	Severity: major Specific problem: The trap indicates the entity is forced to power off Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm indicates the entity is forced to power off.\nAlarm is cleared by the system.\nReason: hh3cEntityExtForcedPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1315 IK8457342

Alarm	Attributes	Applicable major release
Name: IK8457342 (9265) Type: equipmentAlarm Package: lmg.IK8457342 Raised on class: lmg.FRU	Severity: major Specific problem: The trap indicates a fault occures on the specified entity Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm indicates a fault occures on the specified entity.\nAlarm is cleared by the system.\nReason: hh3cEntityExtFaultAlarmOn		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1316 IK8457344

Alarm	Attributes	Applicable major release
Name: IK8457344 (9266) Type: equipmentAlarm Package: lmg.IK8457344 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExtResourceLack Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm indicates that a kind of resource is not enough on the specified entity.\nAlarm is cleared by the system.\nReason: hh3cEntityExtResourceLack		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1317 IK8457346

Alarm	Attributes	Applicable major release
Name: IK8457346 (7131) Type: environmentalAlarm Package: lmg.IK8457346 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExtTemperatureLower Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm indicates the temperature of a specified entity is under the lower threshold. In this condition, user should check the status and the environment of the entity, sometimes it goes wrong for some reason.\nAlarm is cleared by the system.\nReason: hh3cEntityExtTemperatureLower		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1318 IK8457347

Alarm	Attributes	Applicable major release
Name: IK8457347 (7132) Type: environmentalAlarm Package: lmg.IK8457347 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: hh3cEntityExtTemperatureTooUp Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: The alarm indicates the temperature of a specified entity exceeded the shutdown threshold.\nAlarm to be cleared by the operator at the management system.\nReason: hh3cEntityExtTemperatureTooUp		
Remedial action: Check the status and the environment of the entity, sometimes it goes wrong for some reason.		

Table 27-1319 IK8457349

Alarm	Attributes	Applicable major release
Name: IK8457349 (9267) Type: equipmentAlarm Package: lmg.IK8457349 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cEntityExternalAlarmOccur Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: The alarm is generated when the monitored device connected to the specified entity fails.\nAlarm is cleared by the system.\nReason: hh3cEntityExternalAlarmOccur		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1320 IK8457354

Alarm	Attributes	Applicable major release
Name: IK8457354 (7133) Type: communicationsAlarm Package: lmg.IK8457354 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: hh3cEntityExtECCParityAlarm Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The alarm indicates the ECC(Error Correction Code) parity error alarm.\nAlarm to be cleared by the operator at the management system.\nReason: hh3cEntityExtECCParityAlarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1321 IK8457364

Alarm	Attributes	Applicable major release
Name: IK8457364 (9268) Type: communicationsAlarm Package: lmg.IK8457364 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cAggPortInactiveNotification2 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This event will be triggered whenever the port in aggregator is made inactive.\nAlarm is cleared by the system.\nReason: hh3cAggPortInactiveNotification2		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1322 IK8457366

Alarm	Attributes	Applicable major release
Name: IK8457366 (9269) Type: equipmentAlarm Package: lmg.IK8457366 Raised on class: lmg.FRU	Severity: major Specific problem: Trap message is generated when the interface is looped Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Trap message is generated when the interface is looped.\nAlarm is cleared by the system.\nReason: hh3cLpbkdtTrapLoopbacked		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1323 IK8457368

Alarm	Attributes	Applicable major release
Name: IK8457368 (9270) Type: equipmentAlarm Package: lmg.IK8457368 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cLpbkdtTrapPerVlanLoopbacked Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Trap message is generated when the interface is looped in the VLAN.\nAlarm is cleared by the system.\nReason: hh3cLpbkdtTrapPerVlanLoopbacked		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1324 IK8457370

Alarm	Attributes	Applicable major release
Name: IK8457370 (9271) Type: communicationsAlarm Package: lmg.IK8457370 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cSlaveSwitchOver Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: An hh3cSlaveSwitchOver alarm signifies that the action of standby mpu switching to master has completed.\nAlarm is cleared by the system.\nReason: hh3cSlaveSwitchOver		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1325 IK8457377

Alarm	Attributes	Applicable major release
Name: IK8457377 (7134) Type: equipmentAlarm Package: lmg.IK8457377 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cpowerfailure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Power supply failure\nAlarm is cleared by the system.\nReason: hh3cpowerfailure		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1326 IK8457381

Alarm	Attributes	Applicable major release
Name: IK8457381 (9272) Type: equipmentAlarm Package: lmg.IK8457381 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cPowerRemoved Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Power removed\nAlarm is cleared by the system.\nReason: hh3cPowerRemoved		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1327 IK8457386

Alarm	Attributes	Applicable major release
Name: IK8457386 (7135) Type: equipmentAlarm Package: lmg.IK8457386 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cBoardFailure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1327 IK8457386 (continued)

Alarm	Attributes	Applicable major release
Description: Board failed\nAlarm is cleared by the system.\nReason: hh3cBoardFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1328 IK8457390

Alarm	Attributes	Applicable major release
Name: IK8457390 (9273) Type: environmentalAlarm Package: Img.IK8457390 Raised on class: Img.FRU	Severity: major Specific problem: hh3cBoardTemperatureLower Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: Board temperature low\nAlarm is cleared by the system.\nReason: hh3cBoardTemperatureLower		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1329 IK8457391

Alarm	Attributes	Applicable major release
Name: IK8457391 (7136) Type: environmentalAlarm Package: Img.IK8457391 Raised on class: Img.FRU	Severity: major Specific problem: hh3cBoardTemperatureHigher Implicitly cleared: true Default probable cause: highTemperature	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Board temperature high\nAlarm is cleared by the system.\nReason: hh3cBoardTemperatureHigher		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1330 IK8457394

Alarm	Attributes	Applicable major release
Name: IK8457394 (7137) Type: equipmentAlarm Package: Img.IK8457394 Raised on class: Img.LMGMngElement	Severity: major Specific problem: hh3cLoadFailure Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Board load failure\nAlarm to be cleared by the operator at the management system.\nReason: hh3cLoadFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1331 IK8457396

Alarm	Attributes	Applicable major release
Name: IK8457396 (9274) Type: equipmentAlarm Package: lmg.IK8457396 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cBackBoardModeSetFuilure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Back board mode set failure\nAlarm is cleared by the system.\nReason: hh3cBackBoardModeSetFuilure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1332 IK8457404

Alarm	Attributes	Applicable major release
Name: IK8457404 (9275) Type: equipmentAlarm Package: lmg.IK8457404 Raised on class: lmg.FRU	Severity: major Specific problem: hh3cStormRising Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm message is generated when any type of the flux exceeds its upper limit on a port.\nAlarm is cleared by the system.\nReason: hh3cStormRising		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1333 IK8457480

Alarm	Attributes	Applicable major release
Name: IK8457480 (9276) Type: processingErrorAlarm Package: lmg.IK8457480 Raised on class: lmg.FRU	Severity: critical Specific problem: N The device's health has changed to Non-Recoverable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: N The device's health has changed to Non-Recoverable.\nAlarm is cleared by the system.\nReason: hpHttpMgNonRecoverableHealthTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1334 IK8457481

Alarm	Attributes	Applicable major release
Name: IK8457481 (10486) Type: equipmentAlarm Package: lmg.IK8457481 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-1334 IK8457481 (continued)

Alarm	Attributes	Applicable major release
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.		
Remedial action: No action is required.		

Table 27-1335 IK8457482

Alarm	Attributes	Applicable major release
Name: IK8457482 (10487) Type: equipmentAlarm Package: Img.IK8457482 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.		
Remedial action: No action is required.		

Table 27-1336 IK8457483

Alarm	Attributes	Applicable major release
Name: IK8457483 (10488) Type: equipmentAlarm Package: Img.IK8457483 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.		
Remedial action: No action is required.		

Table 27-1337 IK8457484

Alarm	Attributes	Applicable major release
Name: IK8457484 (10489) Type: equipmentAlarm Package: Img.IK8457484 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.		
Remedial action: No action is required.		

Table 27-1338 IK8457485

Alarm	Attributes	Applicable major release
Name: IK8457485 (10490) Type: equipmentAlarm Package: lmg.IK8457485 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.		
Remedial action: No action is required.		

Table 27-1339 IK8457486

Alarm	Attributes	Applicable major release
Name: IK8457486 (10491) Type: equipmentAlarm Package: lmg.IK8457486 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-1340 IK8457487

Alarm	Attributes	Applicable major release
Name: IK8457487 (10492) Type: equipmentAlarm Package: lmg.IK8457487 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-1341 IK8457488

Alarm	Attributes	Applicable major release
Name: IK8457488 (10493) Type: equipmentAlarm Package: lmg.IK8457488 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.		

Table 27-1341 IK8457488 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1342 IK8457489

Alarm	Attributes	Applicable major release
Name: IK8457489 (10494) Type: equipmentAlarm Package: Img.IK8457489 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-1343 IK8457490

Alarm	Attributes	Applicable major release
Name: IK8457490 (10495) Type: equipmentAlarm Package: Img.IK8457490 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-1344 IK8457491

Alarm	Attributes	Applicable major release
Name: IK8457491 (10496) Type: equipmentAlarm Package: Img.IK8457491 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-1345 IK8457492

Alarm	Attributes	Applicable major release
Name: IK8457492 (10497) Type: equipmentAlarm Package: lmg.IK8457492 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: High Priority Alert Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A high priority alert has occurred.		
Remedial action: No action is required.		

Table 27-1346 IK8457493

Alarm	Attributes	Applicable major release
Name: IK8457493 (10498) Type: equipmentAlarm Package: lmg.IK8457493 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Medium Priority Alert Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A medium priority alert has occurred.		
Remedial action: No action is required.		

Table 27-1347 IK8457494

Alarm	Attributes	Applicable major release
Name: IK8457494 (10499) Type: equipmentAlarm Package: lmg.IK8457494 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Low Priority Alert Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A low priority alert has occurred.		
Remedial action: No action is required.		

Table 27-1348 IK8457495

Alarm	Attributes	Applicable major release
Name: IK8457495 (10500) Type: equipmentAlarm Package: lmg.IK8457495 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: DMI Non-Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent whenever a DMI Indication occurs which is Non-Critical level.		
Remedial action: No action is required.		

Table 27-1349 IK8457496

Alarm	Attributes	Applicable major release
Name: IK8457496 (10501) Type: equipmentAlarm Package: Img.IK8457496 Raised on class: Img.FRU	Severity: indeterminate Specific problem: DMI Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent whenever a DMI Indication occurs which is Critical level.		
Remedial action: No action is required.		

Table 27-1350 IK8457497

Alarm	Attributes	Applicable major release
Name: IK8457497 (10502) Type: equipmentAlarm Package: Img.IK8457497 Raised on class: Img.FRU	Severity: indeterminate Specific problem: DMI Non-Recoverable trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent whenever a DMI Indication occurs which is Non-Recoverable level.		
Remedial action: No action is required.		

Table 27-1351 IK8457498

Alarm	Attributes	Applicable major release
Name: IK8457498 (10503) Type: equipmentAlarm Package: Img.IK8457498 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A critical alarm has occurred.		
Remedial action: No action is required.		

Table 27-1352 IK8457500

Alarm	Attributes	Applicable major release
Name: IK8457500 (10504) Type: equipmentAlarm Package: Img.IK8457500 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes degraded.		
Remedial action: No action is required.		

Table 27-1353 IK8457501

Alarm	Attributes	Applicable major release
Name: IK8457501 (10505) Type: equipmentAlarm Package: lmg.IK8457501 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes failed.		
Remedial action: No action is required.		

Table 27-1354 IK8457502

Alarm	Attributes	Applicable major release
Name: IK8457502 (10506) Type: equipmentAlarm Package: lmg.IK8457502 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes degraded.		
Remedial action: No action is required.		

Table 27-1355 IK8457503

Alarm	Attributes	Applicable major release
Name: IK8457503 (10507) Type: equipmentAlarm Package: lmg.IK8457503 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes failed.		
Remedial action: No action is required.		

Table 27-1356 IK8457504

Alarm	Attributes	Applicable major release
Name: IK8457504 (10508) Type: equipmentAlarm Package: lmg.IK8457504 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes degraded.		

Table 27-1356 IK8457504 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1357 IK8457505

Alarm	Attributes	Applicable major release
Name: IK8457505 (10509) Type: equipmentAlarm Package: Img.IK8457505 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes failed.		
Remedial action: No action is required.		

Table 27-1358 IK8457506

Alarm	Attributes	Applicable major release
Name: IK8457506 (10510) Type: equipmentAlarm Package: Img.IK8457506 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-1359 IK8457507

Alarm	Attributes	Applicable major release
Name: IK8457507 (10511) Type: equipmentAlarm Package: Img.IK8457507 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Information Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An informational alarm has occurred.		
Remedial action: No action is required.		

Table 27-1360 IK8457508

Alarm	Attributes	Applicable major release
Name: IK8457508 (10512) Type: equipmentAlarm Package: lmg.IK8457508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1361 IK8457509

Alarm	Attributes	Applicable major release
Name: IK8457509 (10513) Type: equipmentAlarm Package: lmg.IK8457509 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-1362 IK8457510

Alarm	Attributes	Applicable major release
Name: IK8457510 (10514) Type: equipmentAlarm Package: lmg.IK8457510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: External Array Redundant Controller Active. This event signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.		
Remedial action: No action is required.		

Table 27-1363 IK8457511

Alarm	Attributes	Applicable major release
Name: IK8457511 (10515) Type: equipmentAlarm Package: lmg.IK8457511 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1364 IK8457512

Alarm	Attributes	Applicable major release
Name: IK8457512 (10516) Type: equipmentAlarm Package: lmg.IK8457512 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-1365 IK8457513

Alarm	Attributes	Applicable major release
Name: IK8457513 (10517) Type: equipmentAlarm Package: lmg.IK8457513 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log		
Remedial action: No action is required.		

Table 27-1366 IK8457514

Alarm	Attributes	Applicable major release
Name: IK8457514 (10518) Type: equipmentAlarm Package: lmg.IK8457514 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.		
Remedial action: No action is required.		

Table 27-1367 IK8457515

Alarm	Attributes	Applicable major release
Name: IK8457515 (10519) Type: equipmentAlarm Package: lmg.IK8457515 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-1368 IK8457516

Alarm	Attributes	Applicable major release
Name: IK8457516 (10520) Type: equipmentAlarm Package: lmg.IK8457516 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-1369 IK8457517

Alarm	Attributes	Applicable major release
Name: IK8457517 (10521) Type: equipmentAlarm Package: lmg.IK8457517 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-1370 IK8457518

Alarm	Attributes	Applicable major release
Name: IK8457518 (10522) Type: equipmentAlarm Package: Img.IK8457518 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-1371 IK8457519

Alarm	Attributes	Applicable major release
Name: IK8457519 (10523) Type: equipmentAlarm Package: Img.IK8457519 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.		
Remedial action: No action is required.		

Table 27-1372 IK8457520

Alarm	Attributes	Applicable major release
Name: IK8457520 (10524) Type: equipmentAlarm Package: Img.IK8457520 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.		
Remedial action: No action is required.		

Table 27-1373 IK8457521

Alarm	Attributes	Applicable major release
Name: IK8457521 (10525) Type: equipmentAlarm Package: Img.IK8457521 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG

Table 27-1373 IK8457521 (continued)

Alarm	Attributes	Applicable major release
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.		
Remedial action: No action is required.		

Table 27-1374 IK8457522

Alarm	Attributes	Applicable major release
Name: IK8457522 (10526) Type: equipmentAlarm Package: lmg.IK8457522 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.		
Remedial action: No action is required.		

Table 27-1375 IK8457523

Alarm	Attributes	Applicable major release
Name: IK8457523 (10527) Type: equipmentAlarm Package: lmg.IK8457523 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.		
Remedial action: No action is required.		

Table 27-1376 IK8457524

Alarm	Attributes	Applicable major release
Name: IK8457524 (10528) Type: equipmentAlarm Package: lmg.IK8457524 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.		
Remedial action: No action is required.		

Table 27-1377 IK8457525

Alarm	Attributes	Applicable major release
Name: IK8457525 (10529) Type: equipmentAlarm Package: Img.IK8457525 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.		
Remedial action: No action is required.		

Table 27-1378 IK8457526

Alarm	Attributes	Applicable major release
Name: IK8457526 (10530) Type: equipmentAlarm Package: Img.IK8457526 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.		
Remedial action: No action is required.		

Table 27-1379 IK8457527

Alarm	Attributes	Applicable major release
Name: IK8457527 (10531) Type: equipmentAlarm Package: Img.IK8457527 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.		
Remedial action: No action is required.		

Table 27-1380 IK8457528

Alarm	Attributes	Applicable major release
Name: IK8457528 (10532) Type: equipmentAlarm Package: lmg.IK8457528 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-1381 IK8457529

Alarm	Attributes	Applicable major release
Name: IK8457529 (10533) Type: equipmentAlarm Package: lmg.IK8457529 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-1382 IK8457530

Alarm	Attributes	Applicable major release
Name: IK8457530 (10534) Type: equipmentAlarm Package: lmg.IK8457530 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.		
Remedial action: No action is required.		

Table 27-1383 IK8457531

Alarm	Attributes	Applicable major release
Name: IK8457531 (10535) Type: equipmentAlarm Package: Img.IK8457531 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the configured redundant NIC becomes the active NIC.		
Remedial action: No action is required.		

Table 27-1384 IK8457532

Alarm	Attributes	Applicable major release
Name: IK8457532 (10536) Type: equipmentAlarm Package: Img.IK8457532 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.MG
Description: This event is a send to the user to notify him of a Critical Software Update.		
Remedial action: No action is required.		

Table 27-1385 IK8457533

Alarm	Attributes	Applicable major release
Name: IK8457533 (10537) Type: equipmentAlarm Package: Img.IK8457533 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: Controller Active. This event signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.		
Remedial action: No action is required.		

Table 27-1386 IK8457534

Alarm	Attributes	Applicable major release
Name: IK8457534 (10538) Type: equipmentAlarm Package: Img.IK8457534 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-1386 IK8457534 (continued)

Alarm	Attributes	Applicable major release
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1387 IK8457535

Alarm	Attributes	Applicable major release
Name: IK8457535 (10539) Type: equipmentAlarm Package: lmg.IK8457535 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Accelerator Board Bad Data. This event signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1388 IK8457536

Alarm	Attributes	Applicable major release
Name: IK8457536 (10540) Type: equipmentAlarm Package: lmg.IK8457536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the array accelerator cache board.		
Remedial action: No action is required.		

Table 27-1389 IK8457537

Alarm	Attributes	Applicable major release
Name: IK8457537 (10541) Type: equipmentAlarm Package: lmg.IK8457537 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1390 IK8457538

Alarm	Attributes	Applicable major release
Name: IK8457538 (10542) Type: equipmentAlarm Package: Img.IK8457538 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1391 IK8457539

Alarm	Attributes	Applicable major release
Name: IK8457539 (10543) Type: equipmentAlarm Package: Img.IK8457539 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Cache Module Board Bad Data. This event signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-1392 IK8457540

Alarm	Attributes	Applicable major release
Name: IK8457540 (10544) Type: equipmentAlarm Package: Img.IK8457540 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Cache Module Board Backup Power Source Failed. This event signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-1393 IK8457541

Alarm	Attributes	Applicable major release
Name: IK8457541 (10545) Type: equipmentAlarm Package: lmg.IK8457541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-1394 IK8457542

Alarm	Attributes	Applicable major release
Name: IK8457542 (10546) Type: equipmentAlarm Package: lmg.IK8457542 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-1395 IK8457543

Alarm	Attributes	Applicable major release
Name: IK8457543 (10547) Type: equipmentAlarm Package: lmg.IK8457543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.		
Remedial action: No action is required.		

Table 27-1396 IK8457544

Alarm	Attributes	Applicable major release
Name: IK8457544 (10548) Type: equipmentAlarm Package: Img.IK8457544 Raised on class: Img.FRU	Severity: indeterminate Specific problem: cpqIoDrvNonWritableTrap Implicitly cleared: true Default probable cause: inputOutputDeviceError	Release: • LR16.1.MG
Description: IO Drive is not writeable due to excessive wear This event signifies that IO Drive configured with system is not writeable due to excessive wear.		
Remedial action: No action is required.		

Table 27-1397 IK8457545

Alarm	Attributes	Applicable major release
Name: IK8457545 (10549) Type: equipmentAlarm Package: Img.IK8457545 Raised on class: Img.FRU	Severity: indeterminate Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.		
Remedial action: No action is required.		

Table 27-1398 IK8457546

Alarm	Attributes	Applicable major release
Name: IK8457546 (10550) Type: equipmentAlarm Package: Img.IK8457546 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to failed. This event signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-1399 IK8457547

Alarm	Attributes	Applicable major release
Name: IK8457547 (10551) Type: equipmentAlarm Package: lmg.IK8457547 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to degraded. This event signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-1400 IK8457548

Alarm	Attributes	Applicable major release
Name: IK8457548 (10552) Type: equipmentAlarm Package: lmg.IK8457548 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to failed. This event signifies that a power supply has failed.		
Remedial action: No action is required.		

Table 27-1401 IK8457549

Alarm	Attributes	Applicable major release
Name: IK8457549 (10553) Type: equipmentAlarm Package: lmg.IK8457549 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to degraded. This event signifies that a power supply has degraded.		
Remedial action: No action is required.		

Table 27-1402 IK8457550

Alarm	Attributes	Applicable major release
Name: IK8457550 (10554) Type: equipmentAlarm Package: lmg.IK8457550 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem is no longer in a redundant state.		

Table 27-1402 IK8457550 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1403 IK8457551

Alarm	Attributes	Applicable major release
Name: IK8457551 (10555) Type: equipmentAlarm Package: lmg.IK8457551 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power supply detected an input line voltage problem.		
Remedial action: No action is required.		

Table 27-1404 IK8457552

Alarm	Attributes	Applicable major release
Name: IK8457552 (10556) Type: equipmentAlarm Package: lmg.IK8457552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem overload condition.		
Remedial action: No action is required.		

Table 27-1405 IK8457553

Alarm	Attributes	Applicable major release
Name: IK8457553 (10557) Type: equipmentAlarm Package: lmg.IK8457553 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.		
Remedial action: No action is required.		

Table 27-1406 IK8457554

Alarm	Attributes	Applicable major release
Name: IK8457554 (10558) Type: equipmentAlarm Package: lmg.IK8457554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.		
Remedial action: No action is required.		

Table 27-1407 IK8457555

Alarm	Attributes	Applicable major release
Name: IK8457555 (10559) Type: equipmentAlarm Package: lmg.IK8457555 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.		
Remedial action: No action is required.		

Table 27-1408 IK8457556

Alarm	Attributes	Applicable major release
Name: IK8457556 (10560) Type: equipmentAlarm Package: lmg.IK8457556 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-1409 IK8457557

Alarm	Attributes	Applicable major release
Name: IK8457557 (10561) Type: equipmentAlarm Package: lmg.IK8457557 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG

Table 27-1409 IK8457557 (continued)

Alarm	Attributes	Applicable major release
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-1410 IK8457558

Alarm	Attributes	Applicable major release
Name: IK8457558 (10562) Type: equipmentAlarm Package: Img.IK8457558 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Fuse open. The fuse has been tripped.		
Remedial action: No action is required.		

Table 27-1411 IK8457559

Alarm	Attributes	Applicable major release
Name: IK8457559 (10563) Type: equipmentAlarm Package: Img.IK8457559 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.		
Remedial action: No action is required.		

Table 27-1412 IK8457560

Alarm	Attributes	Applicable major release
Name: IK8457560 (10564) Type: equipmentAlarm Package: Img.IK8457560 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.		
Remedial action: No action is required.		

Table 27-1413 IK8457561

Alarm	Attributes	Applicable major release
Name: IK8457561 (10565) Type: equipmentAlarm Package: Img.IK8457561 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.		
Remedial action: No action is required.		

Table 27-1414 IK8457562

Alarm	Attributes	Applicable major release
Name: IK8457562 (10566) Type: equipmentAlarm Package: Img.IK8457562 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.		
Remedial action: No action is required.		

Table 27-1415 IK8457563

Alarm	Attributes	Applicable major release
Name: IK8457563 (10567) Type: equipmentAlarm Package: Img.IK8457563 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.		
Remedial action: No action is required.		

Table 27-1416 IK8457564

Alarm	Attributes	Applicable major release
Name: IK8457564 (10568) Type: equipmentAlarm Package: Img.IK8457564 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG

Table 27-1416 IK8457564 (continued)

Alarm	Attributes	Applicable major release
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.		
Remedial action: No action is required.		

Table 27-1417 IK8457565

Alarm	Attributes	Applicable major release
Name: IK8457565 (10569) Type: equipmentAlarm Package: Img.IK8457565 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.		
Remedial action: No action is required.		

Table 27-1418 IK8457566

Alarm	Attributes	Applicable major release
Name: IK8457566 (10570) Type: equipmentAlarm Package: Img.IK8457566 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.		
Remedial action: No action is required.		

Table 27-1419 IK8457567

Alarm	Attributes	Applicable major release
Name: IK8457567 (10571) Type: equipmentAlarm Package: Img.IK8457567 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper		
Remedial action: No action is required.		

Table 27-1420 IK8457568

Alarm	Attributes	Applicable major release
Name: IK8457568 (10572) Type: equipmentAlarm Package: lmg.IK8457568 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.		
Remedial action: No action is required.		

Table 27-1421 IK8457569

Alarm	Attributes	Applicable major release
Name: IK8457569 (10573) Type: equipmentAlarm Package: lmg.IK8457569 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.		
Remedial action: No action is required.		

Table 27-1422 IK8457570

Alarm	Attributes	Applicable major release
Name: IK8457570 (10574) Type: equipmentAlarm Package: lmg.IK8457570 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.		
Remedial action: No action is required.		

Table 27-1423 IK8457571

Alarm	Attributes	Applicable major release
Name: IK8457571 (10575) Type: equipmentAlarm Package: lmg.IK8457571 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG

Table 27-1423 IK8457571 (continued)

Alarm	Attributes	Applicable major release
Description: FlexFabric Cmdr Power Subsystem Critical trap.		
Remedial action: No action is required.		

Table 27-1424 IK8457572

Alarm	Attributes	Applicable major release
Name: IK8457572 (10576) Type: equipmentAlarm Package: Img.IK8457572 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic WSMAN Major trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Major trap		
Remedial action: No action is required.		

Table 27-1425 IK8457573

Alarm	Attributes	Applicable major release
Name: IK8457573 (10577) Type: equipmentAlarm Package: Img.IK8457573 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic WSMAN Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Critical trap		
Remedial action: No action is required.		

Table 27-1426 IK8457574

Alarm	Attributes	Applicable major release
Name: IK8457574 (10578) Type: equipmentAlarm Package: Img.IK8457574 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-1427 IK8457575

Alarm	Attributes	Applicable major release
Name: IK8457575 (10579) Type: equipmentAlarm Package: Img.IK8457575 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-1428 IK8457576

Alarm	Attributes	Applicable major release
Name: IK8457576 (10580) Type: equipmentAlarm Package: Img.IK8457576 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.		
Remedial action: No action is required.		

Table 27-1429 IK8457577

Alarm	Attributes	Applicable major release
Name: IK8457577 (10581) Type: equipmentAlarm Package: Img.IK8457577 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-1430 IK8457578

Alarm	Attributes	Applicable major release
Name: IK8457578 (10582) Type: equipmentAlarm Package: Img.IK8457578 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.		

Table 27-1430 IK8457578 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1431 IK8457579

Alarm	Attributes	Applicable major release
Name: IK8457579 (10583) Type: equipmentAlarm Package: Img.IK8457579 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-1432 IK8457580

Alarm	Attributes	Applicable major release
Name: IK8457580 (10584) Type: equipmentAlarm Package: Img.IK8457580 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.		
Remedial action: No action is required.		

Table 27-1433 IK8457581

Alarm	Attributes	Applicable major release
Name: IK8457581 (10585) Type: equipmentAlarm Package: Img.IK8457581 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.		
Remedial action: No action is required.		

Table 27-1434 IK8457582

Alarm	Attributes	Applicable major release
Name: IK8457582 (10586) Type: equipmentAlarm Package: Img.IK8457582 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-1435 IK8457583

Alarm	Attributes	Applicable major release
Name: IK8457583 (10587) Type: equipmentAlarm Package: Img.IK8457583 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.		
Remedial action: No action is required.		

Table 27-1436 IK8457584

Alarm	Attributes	Applicable major release
Name: IK8457584 (10588) Type: equipmentAlarm Package: Img.IK8457584 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-1437 IK8457585

Alarm	Attributes	Applicable major release
Name: IK8457585 (10589) Type: equipmentAlarm Package: Img.IK8457585 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-1438 IK8457586

Alarm	Attributes	Applicable major release
Name: IK8457586 (10590) Type: equipmentAlarm Package: Img.IK8457586 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-1439 IK8457587

Alarm	Attributes	Applicable major release
Name: IK8457587 (10591) Type: equipmentAlarm Package: Img.IK8457587 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-1440 IK8457588

Alarm	Attributes	Applicable major release
Name: IK8457588 (10592) Type: equipmentAlarm Package: Img.IK8457588 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-1441 IK8457589

Alarm	Attributes	Applicable major release
Name: IK8457589 (10593) Type: equipmentAlarm Package: Img.IK8457589 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-1442 IK8457590

Alarm	Attributes	Applicable major release
Name: IK8457590 (10594) Type: equipmentAlarm Package: Img.IK8457590 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-1443 IK8457591

Alarm	Attributes	Applicable major release
Name: IK8457591 (10595) Type: equipmentAlarm Package: Img.IK8457591 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.		
Remedial action: No action is required.		

Table 27-1444 IK8457592

Alarm	Attributes	Applicable major release
Name: IK8457592 (10596) Type: equipmentAlarm Package: Img.IK8457592 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-1445 IK8457593

Alarm	Attributes	Applicable major release
Name: IK8457593 (10597) Type: equipmentAlarm Package: Img.IK8457593 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG

Table 27-1445 IK8457593 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-1446 IK8457594

Alarm	Attributes	Applicable major release
Name: IK8457594 (10598) Type: equipmentAlarm Package: Img.IK8457594 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-1447 IK8457595

Alarm	Attributes	Applicable major release
Name: IK8457595 (10599) Type: equipmentAlarm Package: Img.IK8457595 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.		
Remedial action: No action is required.		

Table 27-1448 IK8457596

Alarm	Attributes	Applicable major release
Name: IK8457596 (10600) Type: equipmentAlarm Package: Img.IK8457596 Raised on class: Img.FRU	Severity: indeterminate Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.		
Remedial action: No action is required.		

Table 27-1449 IK8457597

Alarm	Attributes	Applicable major release
Name: IK8457597 (10601) Type: equipmentAlarm Package: lmg.IK8457597 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.		
Remedial action: No action is required.		

Table 27-1450 IK8457598

Alarm	Attributes	Applicable major release
Name: IK8457598 (10602) Type: equipmentAlarm Package: lmg.IK8457598 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.		
Remedial action: No action is required.		

Table 27-1451 IK8457599

Alarm	Attributes	Applicable major release
Name: IK8457599 (10603) Type: equipmentAlarm Package: lmg.IK8457599 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.		
Remedial action: No action is required.		

Table 27-1452 IK8457600

Alarm	Attributes	Applicable major release
Name: IK8457600 (10604) Type: equipmentAlarm Package: lmg.IK8457600 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG

Table 27-1452 IK8457600 (continued)

Alarm	Attributes	Applicable major release
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.		
Remedial action: No action is required.		

Table 27-1453 IK8457601

Alarm	Attributes	Applicable major release
Name: IK8457601 (10605) Type: equipmentAlarm Package: Img.IK8457601 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.		
Remedial action: No action is required.		

Table 27-1454 IK8457602

Alarm	Attributes	Applicable major release
Name: IK8457602 (10606) Type: equipmentAlarm Package: Img.IK8457602 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.		
Remedial action: No action is required.		

Table 27-1455 IK8457603

Alarm	Attributes	Applicable major release
Name: IK8457603 (10607) Type: equipmentAlarm Package: Img.IK8457603 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.		
Remedial action: No action is required.		

Table 27-1456 IK8457604

Alarm	Attributes	Applicable major release
Name: IK8457604 (10608) Type: equipmentAlarm Package: lmg.IK8457604 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.		
Remedial action: No action is required.		

Table 27-1457 IK8457605

Alarm	Attributes	Applicable major release
Name: IK8457605 (10609) Type: equipmentAlarm Package: lmg.IK8457605 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.		
Remedial action: No action is required.		

Table 27-1458 IK8457606

Alarm	Attributes	Applicable major release
Name: IK8457606 (10610) Type: equipmentAlarm Package: lmg.IK8457606 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.		
Remedial action: No action is required.		

Table 27-1459 IK8457607

Alarm	Attributes	Applicable major release
Name: IK8457607 (10611) Type: equipmentAlarm Package: lmg.IK8457607 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A storage system power supply status has been set to degraded.		
Remedial action: No action is required.		

Table 27-1460 IK8500002

Alarm	Attributes	Applicable major release
Name: IK8500002 (7138) Type: environmentalAlarm Package: lmg.IK8500002 Raised on class: lmg.UPlane	Severity: warning Specific problem: Temperature Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Temperature exceeds the max user temperature level. Alarm is cleared by the system.\nReason: Temperature		
Remedial action: Check that the fans of the device are working properly. Check also that configured temperature threshold is not too low (under normal running conditions; approximately 45C when ambiant is at 25C). Finally, check that ambiant temperature is not too high.		

Table 27-1461 IK8500006

Alarm	Attributes	Applicable major release
Name: IK8500006 (7139) Type: communicationsAlarm Package: lmg.IK8500006 Raised on class: lmg.UPlane	Severity: major Specific problem: VRRP failure Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: VRRP Failure Alarm ON. Alarm is cleared by the system.\nReason: VRRP failure		
Remedial action: Connect another user-plane device with the same VRRP Id and parameters on the appropriate IP interface.		

Table 27-1462 IK8500103

Alarm	Attributes	Applicable major release
Name: IK8500103 (7140) Type: communicationsAlarm Package: lmg.IK8500103 Raised on class: lmg.UPlane	Severity: major Specific problem: NTP Server Locked Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: NTP server unreachable. Alarm is cleared by the system.\nReason: NTP Server Locked		
Remedial action: Connect a NTP server with an appropriate IP address on OA&M network (reachable by the user-plane on eth0)		

Table 27-1463 IK8500501

Alarm	Attributes	Applicable major release
Name: IK8500501 (7141) Type: communicationsAlarm Package: lmg.IK8500501 Raised on class: lmg.UPlane	Severity: critical Specific problem: Internal 10MHz not locked Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Internal 10MHz OCXO is not locked. Alarm is cleared by the system.\nReason: Internal 10MHz not locked		
Remedial action: Verify the quality of the GPS antenna connection.		

Table 27-1464 IK8500503

Alarm	Attributes	Applicable major release
Name: IK8500503 (7142) Type: communicationsAlarm Package: lmg.IK8500503 Raised on class: lmg.UPlane	Severity: major Specific problem: Internal GPS not locked Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Internal GPS is not locked. Alarm is cleared by the system.\nReason: Internal GPS not locked		
Remedial action: Connect a GPS antenna (3. 3V) on the appropriate device input (TNC connector).		

Table 27-1465 IK8501061

Alarm	Attributes	Applicable major release
Name: IK8501061 (7143) Type: communicationsAlarm Package: lmg.IK8501061 Raised on class: lmg.UPlane	Severity: critical Specific problem: IP Data 1 link Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1465 IK8501061 (continued)

Alarm	Attributes	Applicable major release
Description: IP Data 1 link failure. Alarm is cleared by the system.\nReason: IP Data 1 link		
Remedial action: Connect eth2 ethernet port to the production network.		

Table 27-1466 IK8501062

Alarm	Attributes	Applicable major release
Name: IK8501062 (7144) Type: communicationsAlarm Package: Img.IK8501062 Raised on class: Img.UPlane	Severity: minor Specific problem: IP Data 2 link Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: IP Data 2 link failure. Alarm is cleared by the system.\nReason: IP Data 2 link		
Remedial action: Connect eth3 ethernet port to the production network.		

Table 27-1467 IK8505555

Alarm	Attributes	Applicable major release
Name: IK8505555 (7145) Type: communicationsAlarm Package: Img.IK8505555 Raised on class: Img.UPlane	Severity: major Specific problem: Output Overflow Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Output Overflow. Alarm is cleared by the system.\nReason: Output Overflow		
Remedial action: Reduce the overall bit rate of the user-plane by : 1) removing some bearers, 2) removing some multi-unicast outputs, 3) decreasing the GBR parameters for one or several bearers.		

Table 27-1468 IK8505556

Alarm	Attributes	Applicable major release
Name: IK8505556 (7146) Type: communicationsAlarm Package: Img.IK8505556 Raised on class: Img.UPlane	Severity: major Specific problem: MTU of Input Stream Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: MTU of Input Stream. Alarm is cleared by the system.\nReason: MTU of Input Stream		
Remedial action: Reduce the maximum size (in number of bytes) of IP packets at the input of the user-plane.		

Table 27-1469 IK8505557

Alarm	Attributes	Applicable major release
Name: IK8505557 (7147) Type: communicationsAlarm Package: lmg.IK8505557 Raised on class: lmg.UPlane	Severity: major Specific problem: Bearer Output Overflow Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Bearer Output Overflow (please note that BearerId is indicated in case less than 3 bearers are in overflow). Alarm is cleared by the system.\nReason: Bearer Output Overflow		
Remedial action: Reduce the bit rate of the corresponding MBMS bearers (see the list in log file)		

Table 27-1470 IK8505558

Alarm	Attributes	Applicable major release
Name: IK8505558 (7148) Type: communicationsAlarm Package: lmg.IK8505558 Raised on class: lmg.UPlane	Severity: minor Specific problem: Bearer Input Missing Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Bearer Input Missing (please note that BearerId is indicated in case less than 3 bearers are missing). Alarm is cleared by the system.\nReason: Bearer Input Missing		
Remedial action: Check that a corresponding IP stream is available on the production network (Check also for possible VLAN configuration)		

Table 27-1471 IK8510001

Alarm	Attributes	Applicable major release
Name: IK8510001 (9277) Type: processingErrorAlarm Package: lmg.IK8510001 Raised on class: lmg.UPlane	Severity: major Specific problem: NTP Server Locked Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This alarm is raised when SW UPlane looses NTP synchronization. Alarm is cleared by the system.\nReason: NTP Server Locked		
Remedial action: Verify Uplane NTP client configuration		

Table 27-1472 IK8510002

Alarm	Attributes	Applicable major release
Name: IK8510002 (9278) Type: processingErrorAlarm Package: Img.IK8510002 Raised on class: Img.UPlane	Severity: major Specific problem: MTU of Input Stream Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This alarm is raised when some ingress traffic packets are too long to add SYNC header during a specific period. Alarm is cleared by the system.\nReason: MTU of Input Stream		
Remedial action: Reduce the maximum size (in number of bytes) of IP packets at the input of the user-plane		

Table 27-1473 IK8510003

Alarm	Attributes	Applicable major release
Name: IK8510003 (9279) Type: processingErrorAlarm Package: Img.IK8510003 Raised on class: Img.UPlane	Severity: major Specific problem: Bearer Output Overflow Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This alarm is raised when Uplane has a Bearer Output Overflow during a specific period. The output overflow is defined by a percentage. Alarm is cleared by the system.\nReason: Bearer Output Overflow		
Remedial action: Reduce the input rate of the corresponding MBMS bearers		

Table 27-1474 IK8510011

Alarm	Attributes	Applicable major release
Name: IK8510011 (9956) Type: communicationsAlarm Package: Img.IK8510011 Raised on class: Img.UPlane	Severity: major Specific problem: NTP Server Locked Implicitly cleared: true Default probable cause: communicationsReceiveFail-ure	Release: • LR16.1.MG
Description: This alarm is raised when SW UPlane loses NTP synchronization. Alarm is cleared by the system.\nReason: NTP Server Locked		
Remedial action: Verify Uplane NTP client configuration		

Table 27-1475 IK8510012

Alarm	Attributes	Applicable major release
Name: IK8510012 (9957) Type: qualityOfServiceAlarm Package: Img.IK8510012 Raised on class: Img.UPlane	Severity: major Specific problem: MTU of Input Stream Implicitly cleared: true Default probable cause: bandwidthReduced	Release: • LR16.1.MG

Table 27-1475 IK8510012 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when some ingress traffic packets are too long to add SYNC header during a specific period. Alarm is cleared by the system.\nReason: MTU of Input Stream		
Remedial action: Reduce the maximum size (in number of bytes) of IP packets at the input of the user-plane		

Table 27-1476 IK8510013

Alarm	Attributes	Applicable major release
Name: IK8510013 (9958) Type: qualityOfServiceAlarm Package: Img.IK8510013 Raised on class: Img.UPlane	Severity: major Specific problem: Bearer Output Overflow Implicitly cleared: true Default probable cause: bandwidthReduced	Release: • LR16.1.MG
Description: This alarm is raised when Uplane has a Bearer Output Overflow during a specific period. The output overflow is defined by a percentage. Alarm is cleared by the system.\nReason: Bearer Output Overflow		
Remedial action: Reduce the input rate of the corresponding MBMS bearers		

Table 27-1477 IK8550005

Alarm	Attributes	Applicable major release
Name: IK8550005 (7149) Type: processingErrorAlarm Package: Img.IK8550005 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: mcdp alarm trap v1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: mcdp alarm alarm v1.\nAlarm is cleared by the system.\nReason: alarmTrapV1		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1478 IK8550006

Alarm	Attributes	Applicable major release
Name: IK8550006 (7150) Type: processingErrorAlarm Package: Img.IK8550006 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Trap associated to an alarm of the managed element Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Trap associated to an alarm of the managed element.\nAlarm is cleared by the system when the device is restarted.\nReason: alarmTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1479 IK8550007

Alarm	Attributes	Applicable major release
Name: IK8550007 (7151) Type: processingErrorAlarm Package: Img.IK8550007 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: softwareFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Trap associated to an alarm while executing software operation (download, activation, validation, reject, backup).\nAlarm is cleared by the system.\nReason: softwareFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1480 IK8550981

Alarm	Attributes	Applicable major release
Name: IK8550981 (7152) Type: equipmentAlarm Package: Img.IK8550981 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeDegraded		
Remedial action: Make a note of the cluster node name then check the node for the cause of the degraded condition.		

Table 27-1481 IK8550982

Alarm	Attributes	Applicable major release
Name: IK8550982 (7153) Type: equipmentAlarm Package: Img.IK8550982 Raised on class: Img.FilePrepare	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-1482 IK8550983

Alarm	Attributes	Applicable major release
Name: IK8550983 (7154) Type: processingErrorAlarm Package: lmg.IK8550983 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceDegraded		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the degraded condition.		

Table 27-1483 IK8550984

Alarm	Attributes	Applicable major release
Name: IK8550984 (7155) Type: processingErrorAlarm Package: lmg.IK8550984 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-1484 IK8550985

Alarm	Attributes	Applicable major release
Name: IK8550985 (7156) Type: equipmentAlarm Package: lmg.IK8550985 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkDegraded		
Remedial action: Make a note of the cluster network name then check the network for the cause of the degraded condition.		

Table 27-1485 IK8550986

Alarm	Attributes	Applicable major release
Name: IK8550986 (7157) Type: equipmentAlarm Package: Img.IK8550986 Raised on class: Img.FilePrepare	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-1486 IK8550987

Alarm	Attributes	Applicable major release
Name: IK8550987 (7158) Type: environmentalAlarm Package: Img.IK8550987 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The temperature at rack sensor 1 is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmTemp1		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1487 IK8550988

Alarm	Attributes	Applicable major release
Name: IK8550988 (7159) Type: environmentalAlarm Package: Img.IK8550988 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The temperature at rack sensor 2 is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmTemp2		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1488 IK8550989

Alarm	Attributes	Applicable major release
Name: IK8550989 (7160) Type: environmentalAlarm Package: Img.IK8550989 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG

Table 27-1488 IK8550989 (continued)

Alarm	Attributes	Applicable major release
Description: The status of Fan 1 has changed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmFan1		
Remedial action: Refer to Trap Details for more information.		

Table 27-1489 IK8550990

Alarm	Attributes	Applicable major release
Name: IK8550990 (7161) Type: environmentalAlarm Package: lmg.IK8550990 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: The status of Fan 2 has changed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmFan2		
Remedial action: Refer to Trap Details for more information.		

Table 27-1490 IK8550991

Alarm	Attributes	Applicable major release
Name: IK8550991 (7162) Type: equipmentAlarm Package: lmg.IK8550991 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The AC voltage of the rack is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmVoltage		
Remedial action: Check the incoming power source and ensure all cables are inserted correctly.		

Table 27-1491 IK8550992

Alarm	Attributes	Applicable major release
Name: IK8550992 (7163) Type: environmentalAlarm Package: lmg.IK8550992 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: humidityUnacceptable	Release: • LR14.3.MG
Description: The humidity of the rack is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmHumidity		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1492 IK8550993

Alarm	Attributes	Applicable major release
Name: IK8550993 (7164) Type: environmentalAlarm Package: Img.IK8550993 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #1).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput1		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1493 IK8550994

Alarm	Attributes	Applicable major release
Name: IK8550994 (7165) Type: environmentalAlarm Package: Img.IK8550994 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #2).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput2		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1494 IK8550995

Alarm	Attributes	Applicable major release
Name: IK8550995 (7166) Type: environmentalAlarm Package: Img.IK8550995 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #3).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput3		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1495 IK8550996

Alarm	Attributes	Applicable major release
Name: IK8550996 (7167) Type: environmentalAlarm Package: Img.IK8550996 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG

Table 27-1495 IK8550996 (continued)

Alarm	Attributes	Applicable major release
Description: The door or sidepanel of the rack has been opened (access point #4).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput4		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1496 IK8550997

Alarm	Attributes	Applicable major release
Name: IK8550997 (7168) Type: processingErrorAlarm Package: lmg.IK8550997 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Rack door lock #1 alarm.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock1		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1497 IK8550998

Alarm	Attributes	Applicable major release
Name: IK8550998 (7169) Type: processingErrorAlarm Package: lmg.IK8550998 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Rack door lock #2 alarm.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock2		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1498 IK8550999

Alarm	Attributes	Applicable major release
Name: IK8550999 (7170) Type: environmentalAlarm Package: lmg.IK8550999 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: smoke	Release: • LR14.3.MG
Description: The rack smoke detector has detected smoke.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmSmoke		
Remedial action: Investigate rack for an over temperature condition and refer to Trap Details for more information.		

Table 27-1499 IK8551000

Alarm	Attributes	Applicable major release
Name: IK8551000 (7171) Type: environmentalAlarm Package: lmg.IK8551000 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: excessiveVibration	Release: • LR14.3.MG
Description: The rack shock detector has detected a vibration to the rack.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmShock		
Remedial action: Investigate rack.		

Table 27-1500 IK8551001

Alarm	Attributes	Applicable major release
Name: IK8551001 (7172) Type: equipmentAlarm Package: lmg.IK8551001 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The rack auxiliary alarm input #1 has been triggered.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmAux1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1501 IK8551002

Alarm	Attributes	Applicable major release
Name: IK8551002 (7173) Type: equipmentAlarm Package: lmg.IK8551002 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The rack auxiliary alarm input #2 has been triggered.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmAux2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1502 IK8551003

Alarm	Attributes	Applicable major release
Name: IK8551003 (7174) Type: communicationsAlarm Package: lmg.IK8551003 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-1502 IK8551003 (continued)

Alarm	Attributes	Applicable major release
Description: Alarm 1, set from Network management\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarm1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1503 IK8551004

Alarm	Attributes	Applicable major release
Name: IK8551004 (7175) Type: communicationsAlarm Package: lmg.IK8551004 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Alarm 2, set from Network management\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarm2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1504 IK8551005

Alarm	Attributes	Applicable major release
Name: IK8551005 (7176) Type: processingErrorAlarm Package: lmg.IK8551005 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm of device Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: The rack door locking device #1 has failed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock1Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-1505 IK8551006

Alarm	Attributes	Applicable major release
Name: IK8551006 (7177) Type: processingErrorAlarm Package: lmg.IK8551006 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm of device Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: The rack door locking device #2 has failed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock2Dev		

Table 27-1505 IK8551006 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-1506 IK8551008

Alarm	Attributes	Applicable major release
Name: IK8551008 (7178) Type: equipmentAlarm Package: Img.IK8551008 Raised on class: Img.FilePrepare	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-1507 IK8551010

Alarm	Attributes	Applicable major release
Name: IK8551010 (7179) Type: equipmentAlarm Package: Img.IK8551010 Raised on class: Img.FilePrepare	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-1508 IK8551013

Alarm	Attributes	Applicable major release
Name: IK8551013 (7180) Type: equipmentAlarm Package: Img.IK8551013 Raised on class: Img.FilePrepare	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-1509 IK8551015

Alarm	Attributes	Applicable major release
Name: IK8551015 (7181) Type: equipmentAlarm Package: lmg.IK8551015 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveReducedTrap		
Remedial action: Replace the failed disk device; add a spare to the system to cause a reconstruct.		

Table 27-1510 IK8551018

Alarm	Attributes	Applicable major release
Name: IK8551018 (7182) Type: processingErrorAlarm Package: lmg.IK8551018 Raised on class: lmg.FilePrepare	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-1511 IK8551023

Alarm	Attributes	Applicable major release
Name: IK8551023 (7183) Type: processingErrorAlarm Package: lmg.IK8551023 Raised on class: lmg.FilePrepare	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-1512 IK8551028

Alarm	Attributes	Applicable major release
Name: IK8551028 (7184) Type: environmentalAlarm Package: lmg.IK8551028 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-1512 IK8551028 (continued)

Alarm	Attributes	Applicable major release
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUFanFailureTrap		
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-1513 IK8551030

Alarm	Attributes	Applicable major release
Name: IK8551030 (7185) Type: equipmentAlarm Package: lmg.IK8551030 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-1514 IK8551032

Alarm	Attributes	Applicable major release
Name: IK8551032 (7186) Type: equipmentAlarm Package: lmg.IK8551032 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUTemperature-WarningTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-1515 IK8551033

Alarm	Attributes	Applicable major release
Name: IK8551033 (7187) Type: equipmentAlarm Package: lmg.IK8551033 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		

Table 27-1515 IK8551033 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-1516 IK8551035

Alarm	Attributes	Applicable major release
Name: IK8551035 (7188) Type: environmentalAlarm Package: lmg.IK8551035 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabFanFailureTrap		
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-1517 IK8551037

Alarm	Attributes	Applicable major release
Name: IK8551037 (7189) Type: equipmentAlarm Package: lmg.IK8551037 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-1518 IK8551039

Alarm	Attributes	Applicable major release
Name: IK8551039 (7190) Type: environmentalAlarm Package: lmg.IK8551039 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabTemperatureWarningTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-1519 IK8551040

Alarm	Attributes	Applicable major release
Name: IK8551040 (7191) Type: environmentalAlarm Package: lmg.IK8551040 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-1520 IK8551059

Alarm	Attributes	Applicable major release
Name: IK8551059 (7192) Type: equipmentAlarm Package: lmg.IK8551059 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-1521 IK8551060

Alarm	Attributes	Applicable major release
Name: IK8551060 (7193) Type: environmentalAlarm Package: lmg.IK8551060 Raised on class: lmg.FilePrepare	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1522 IK8551067

Alarm	Attributes	Applicable major release
Name: IK8551067 (7194) Type: equipmentAlarm Package: lmg.IK8551067 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Fibre Channel Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Fibre Channel Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqFcTapeDriveCleanTapeReplace		
Remedial action: Replace the failing fibre channel drive cleaning tape		

Table 27-1523 IK8551068

Alarm	Attributes	Applicable major release
Name: IK8551068 (7195) Type: processingErrorAlarm Package: lmg.IK8551068 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Redundant Controller Active. This alarm signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-1524 IK8551072

Alarm	Attributes	Applicable major release
Name: IK8551072 (7196) Type: equipmentAlarm Package: lmg.IK8551072 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-1525 IK8551073

Alarm	Attributes	Applicable major release
Name: IK8551073 (7197) Type: environmentalAlarm Package: Img.IK8551073 Raised on class: Img.FilePrepare	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1526 IK8551078

Alarm	Attributes	Applicable major release
Name: IK8551078 (7198) Type: processingErrorAlarm Package: Img.IK8551078 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: External Tape Drive Cleaning Required Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: External Tape Drive Cleaning Required. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm to be cleared by the operator at the management system.\nReason: cpqExtTapeDriveCleaningRequired		
Remedial action: a External Tape Drive Cleaning should be installed		

Table 27-1527 IK8551079

Alarm	Attributes	Applicable major release
Name: IK8551079 (7199) Type: equipmentAlarm Package: Img.IK8551079 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: External Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: External Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqExtTapeDriveCleanTapeReplace		
Remedial action: Replace the External Tape Drive Cleaning Tape		

Table 27-1528 IK8551088

Alarm	Attributes	Applicable major release
Name: IK8551088 (9280) Type: environmentalAlarm Package: Img.IK8551088 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHeThermalTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1529 IK8551089

Alarm	Attributes	Applicable major release
Name: IK8551089 (7200) Type: environmentalAlarm Package: Img.IK8551089 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Thermal Status Degraded Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The temperature status has been set to degraded. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeThermalTempDegraded		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1530 IK8551091

Alarm	Attributes	Applicable major release
Name: IK8551091 (9281) Type: environmentalAlarm Package: Img.IK8551091 Raised on class: Img.FilePrepare	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1531 IK8551092

Alarm	Attributes	Applicable major release
Name: IK8551092 (7201) Type: environmentalAlarm Package: Img.IK8551092 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: System Fan Degraded Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: The system fan status has been set to degraded. An optional system fan is not operating normally.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeThermalSystemFanDegraded		
Remedial action: check the system fans		

Table 27-1532 IK8551094

Alarm	Attributes	Applicable major release
Name: IK8551094 (7202) Type: environmentalAlarm Package: Img.IK8551094 Raised on class: Img.FilePrepare	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHeThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1533 IK8551098

Alarm	Attributes	Applicable major release
Name: IK8551098 (7203) Type: equipmentAlarm Package: Img.IK8551098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-1534 IK8551099

Alarm	Attributes	Applicable major release
Name: IK8551099 (7204) Type: equipmentAlarm Package: Img.IK8551099 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Server Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-1534 IK8551099 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply sub-system condition has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeFltTolPwrSupplyDegraded		
Remedial action: check the fault tolerant power supply		

Table 27-1535 IK8551102

Alarm	Attributes	Applicable major release
Name: IK8551102 (7205) Type: environmentalAlarm Package: lmg.IK8551102 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1536 IK8551103

Alarm	Attributes	Applicable major release
Name: IK8551103 (7206) Type: environmentalAlarm Package: lmg.IK8551103 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Temperature Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to degraded. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1537 IK8551105

Alarm	Attributes	Applicable major release
Name: IK8551105 (7207) Type: environmentalAlarm Package: lmg.IK8551105 Raised on class: lmg.FilePrepare	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1537 IK8551105 (continued)

Alarm	Attributes	Applicable major release
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1538 IK8551106

Alarm	Attributes	Applicable major release
Name: IK8551106 (7208) Type: environmentalAlarm Package: Img.IK8551106 Raised on class: Img.FilePrepare	Severity: minor Specific problem: System Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to degraded. An optional system fan is not operating normally.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-1539 IK8551108

Alarm	Attributes	Applicable major release
Name: IK8551108 (7209) Type: environmentalAlarm Package: Img.IK8551108 Raised on class: Img.FilePrepare	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1540 IK8551112

Alarm	Attributes	Applicable major release
Name: IK8551112 (7210) Type: equipmentAlarm Package: Img.IK8551112 Raised on class: Img.FilePrepare	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		

Table 27-1540 IK8551112 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-1541 IK8551113

Alarm	Attributes	Applicable major release
Name: IK8551113 (7211) Type: equipmentAlarm Package: Img.IK8551113 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolPwrSupplyDegraded		
Remedial action: Check the system for a power supply failure. Replace the power supply.		

Table 27-1542 IK8551114

Alarm	Attributes	Applicable major release
Name: IK8551114 (7212) Type: processingErrorAlarm Package: Img.IK8551114 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Corr Mem Errors Require a Replacement Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: A correctable memory log entry indicates a memory module needs to be replaced. The errors have been corrected, but the memory module should be replaced. The error information is reported in the variable cpqHeCorrMemErrDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe3CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module		

Table 27-1543 IK8551116

Alarm	Attributes	Applicable major release
Name: IK8551116 (7213) Type: equipmentAlarm Package: Img.IK8551116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1544 IK8551117

Alarm	Attributes	Applicable major release
Name: IK8551117 (7214) Type: equipmentAlarm Package: Img.IK8551117 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Power Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The Fault Tolerant Power Supplies have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerRedundancyLost		
Remedial action: Check the system power supplies for a failure.		

Table 27-1545 IK8551120

Alarm	Attributes	Applicable major release
Name: IK8551120 (7215) Type: environmentalAlarm Package: Img.IK8551120 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-1546 IK8551121

Alarm	Attributes	Applicable major release
Name: IK8551121 (7216) Type: environmentalAlarm Package: Img.IK8551121 Raised on class: Img.FilePrepare	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1547 IK8551122

Alarm	Attributes	Applicable major release
Name: IK8551122 (7217) Type: environmentalAlarm Package: Img.IK8551122 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Fan Redundancy Lost Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1547 IK8551122 (continued)

Alarm	Attributes	Applicable major release
Description: The Fault Tolerant Fans have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolFanRedundancyLost		
Remedial action: Check the system fans for a failure.		

Table 27-1548 IK8551125

Alarm	Attributes	Applicable major release
Name: IK8551125 (7218) Type: environmentalAlarm Package: Img.IK8551125 Raised on class: Img.FilePrepare	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1549 IK8551126

Alarm	Attributes	Applicable major release
Name: IK8551126 (7219) Type: environmentalAlarm Package: Img.IK8551126 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Thermal Status Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to degraded in the specified chassis and location. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-1550 IK8551128

Alarm	Attributes	Applicable major release
Name: IK8551128 (7220) Type: equipmentAlarm Package: Img.IK8551128 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterDegraded		

Table 27-1550 IK8551128 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check for a failing power converter or for a failed power converter in a redundant pair. Replace the power converter.		

Table 27-1551 IK8551129

Alarm	Attributes	Applicable major release
Name: IK8551129 (7221) Type: equipmentAlarm Package: Img.IK8551129 Raised on class: Img.FilePrepare	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-1552 IK8551130

Alarm	Attributes	Applicable major release
Name: IK8551130 (7222) Type: equipmentAlarm Package: Img.IK8551130 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterRedundancyLost		
Remedial action: Check the power converters in the system for a failure in a redundant pair. Replace the power converter.		

Table 27-1553 IK8551131

Alarm	Attributes	Applicable major release
Name: IK8551131 (7223) Type: communicationsAlarm Package: Img.IK8551131 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3CacheAccelParityError		
Remedial action: Refer to the Integrated Management Log for details on the error. Replace the cache module.		

Table 27-1554 IK8551132

Alarm	Attributes	Applicable major release
Name: IK8551132 (7224) Type: processingErrorAlarm Package: Img.IK8551132 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemOnlineSpareEngaged		
Remedial action: Schedule server down-time to replace the faulty memory.		

Table 27-1555 IK8551134

Alarm	Attributes	Applicable major release
Name: IK8551134 (7225) Type: equipmentAlarm Package: Img.IK8551134 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to degraded for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1556 IK8551135

Alarm	Attributes	Applicable major release
Name: IK8551135 (7226) Type: equipmentAlarm Package: Img.IK8551135 Raised on class: Img.FilePrepare	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1557 IK8551136

Alarm	Attributes	Applicable major release
Name: IK8551136 (7227) Type: processingErrorAlarm Package: Img.IK8551136 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemMirroredMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-1558 IK8551137

Alarm	Attributes	Applicable major release
Name: IK8551137 (7228) Type: processingErrorAlarm Package: Img.IK8551137 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientAdvancedECCMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-1559 IK8551138

Alarm	Attributes	Applicable major release
Name: IK8551138 (7229) Type: processingErrorAlarm Package: Img.IK8551138 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemXorMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-1560 IK8551141

Alarm	Attributes	Applicable major release
Name: IK8551141 (7230) Type: processingErrorAlarm Package: Img.IK8551141 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Replace Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: Corrected Memory Errors Detected. The errors have been corrected, but the memory module should be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe4CorrMemReplaceMemModule		
Remedial action: Replace the memory module.		

Table 27-1561 IK8551142

Alarm	Attributes	Applicable major release
Name: IK8551142 (7231) Type: equipmentAlarm Package: Img.IK8551142 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardRemoved		
Remedial action: Insure the board or cartridge has memory correctly installed and re-insert the memory board or cartridge back into the system.		

Table 27-1562 IK8551144

Alarm	Attributes	Applicable major release
Name: IK8551144 (7232) Type: processingErrorAlarm Package: Img.IK8551144 Raised on class: Img.FilePrepare	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-1563 IK8551148

Alarm	Attributes	Applicable major release
Name: IK8551148 (7233) Type: equipmentAlarm Package: Img.IK8551148 Raised on class: Img.FilePrepare	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-1564 IK8551149

Alarm	Attributes	Applicable major release
Name: IK8551149 (7234) Type: processingErrorAlarm Package: Img.IK8551149 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Replace Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: Corrected \ uncorrected Memory Errors Detected. The errors have been corrected, but the memory module should be replaced. Value 0 for CPU means memory is not Processor based\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe5CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module.		

Table 27-1565 IK8551150

Alarm	Attributes	Applicable major release
Name: IK8551150 (7235) Type: equipmentAlarm Package: Img.IK8551150 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardRemoved		
Remedial action: Insure the board or cartridge or riser has memory correctly installed and re-insert the memory board or cartridge or CPU back into the system.		

Table 27-1566 IK8551152

Alarm	Attributes	Applicable major release
Name: IK8551152 (7236) Type: processingErrorAlarm Package: Img.IK8551152 Raised on class: Img.FilePrepare	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-1567 IK8551153

Alarm	Attributes	Applicable major release
Name: IK8551153 (7237) Type: processingErrorAlarm Package: Img.IK8551153 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemLockStepMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-1568 IK8551154

Alarm	Attributes	Applicable major release
Name: IK8551154 (7238) Type: equipmentAlarm Package: Img.IK8551154 Raised on class: Img.FilePrepare	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-1569 IK8551156

Alarm	Attributes	Applicable major release
Name: IK8551156 (7239) Type: processingErrorAlarm Package: Img.IK8551156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1570 IK8551158

Alarm	Attributes	Applicable major release
Name: IK8551158 (7240) Type: processingErrorAlarm Package: Img.IK8551158 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1571 IK8551160

Alarm	Attributes	Applicable major release
Name: IK8551160 (9282) Type: communicationsAlarm Package: Img.IK8551160 Raised on class: Img.FilePrepare	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-1572 IK8551163

Alarm	Attributes	Applicable major release
Name: IK8551163 (7241) Type: communicationsAlarm Package: lmg.IK8551163 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-1573 IK8551164

Alarm	Attributes	Applicable major release
Name: IK8551164 (7242) Type: communicationsAlarm Package: lmg.IK8551164 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the configured redundant NIC becomes the active NIC.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHo2NicSwitchoverOccurred2		
Remedial action: Examine the network connections and check for a NIC failure.		

Table 27-1574 IK8551168

Alarm	Attributes	Applicable major release
Name: IK8551168 (7243) Type: processingErrorAlarm Package: lmg.IK8551168 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is a send to the user to notify him of a Critical Software Update.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHoCriticalSoftwareUpdateTrap		
Remedial action: Install the required software updates.		

Table 27-1575 IK8551172

Alarm	Attributes	Applicable major release
Name: IK8551172 (7244) Type: qualityOfServiceAlarm Package: lmg.IK8551172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1576 IK8552265

Alarm	Attributes	Applicable major release
Name: IK8552265 (7245) Type: environmentalAlarm Package: lmg.IK8552265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1577 IK8552272

Alarm	Attributes	Applicable major release
Name: IK8552272 (7246) Type: environmentalAlarm Package: lmg.IK8552272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1578 IK8552279

Alarm	Attributes	Applicable major release
Name: IK8552279 (7247) Type: environmentalAlarm Package: lmg.IK8552279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-1579 IK8552281

Alarm	Attributes	Applicable major release
Name: IK8552281 (7248) Type: processingErrorAlarm Package: lmg.IK8552281 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Controller Active. This alarm signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-1580 IK8552284

Alarm	Attributes	Applicable major release
Name: IK8552284 (7249) Type: equipmentAlarm Package: lmg.IK8552284 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa4PhyDrvThreshPassedTrap		
Remedial action: If the physical drive is predicting failure, replace the drive.		

Table 27-1581 IK8552289

Alarm	Attributes	Applicable major release
Name: IK8552289 (7250) Type: equipmentAlarm Package: lmg.IK8552289 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaTapeDriveCleanTapeReplace		
Remedial action: Replace the Tape Drive Cleaning Tape.		

Table 27-1582 IK8552291

Alarm	Attributes	Applicable major release
Name: IK8552291 (7251) Type: equipmentAlarm Package: lmg.IK8552291 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-1583 IK8552292

Alarm	Attributes	Applicable major release
Name: IK8552292 (7252) Type: environmentalAlarm Package: lmg.IK8552292 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-1584 IK8552295

Alarm	Attributes	Applicable major release
Name: IK8552295 (7253) Type: equipmentAlarm Package: Img.IK8552295 Raised on class: Img.FilePrepare	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-1585 IK8552302

Alarm	Attributes	Applicable major release
Name: IK8552302 (7254) Type: equipmentAlarm Package: Img.IK8552302 Raised on class: Img.FilePrepare	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-1586 IK8552304

Alarm	Attributes	Applicable major release
Name: IK8552304 (7255) Type: equipmentAlarm Package: Img.IK8552304 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Cache Module Board Bad Data. This alarm signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-1587 IK8552305

Alarm	Attributes	Applicable major release
Name: IK8552305 (7256) Type: environmentalAlarm Package: Img.IK8552305 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Cache Module Board Backup Power Source Failed. This alarm signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBatteryFailed		
Remedial action: Replace the Backup Power Source.		

Table 27-1588 IK8552309

Alarm	Attributes	Applicable major release
Name: IK8552309 (7257) Type: processingErrorAlarm Package: Img.IK8552309 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-1589 IK8552310

Alarm	Attributes	Applicable major release
Name: IK8552310 (7258) Type: equipmentAlarm Package: Img.IK8552310 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-1590 IK8552315

Alarm	Attributes	Applicable major release
Name: IK8552315 (7259) Type: equipmentAlarm Package: lmg.IK8552315 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: IDE Drive Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: An IDE drive status has been set to degraded.\nAlarm is cleared by the system.\nReason: cpqIdeDriveDegraded		
Remedial action: The drive should be scheduled for replacement. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1591 IK8552317

Alarm	Attributes	Applicable major release
Name: IK8552317 (7260) Type: equipmentAlarm Package: lmg.IK8552317 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqIdeDriveUltraAtaDegraded		
Remedial action: For best performance move Ultra ATA devices to the primary controller and non Ultra ATA devices to the secondary controller. If errors still persist, consider replacing the standard 40-conductor IDE cable with an 80-conductor Ultra ATA cable.		

Table 27-1592 IK8552337

Alarm	Attributes	Applicable major release
Name: IK8552337 (7261) Type: communicationsAlarm Package: lmg.IK8552337 Raised on class: lmg.FilePrepare	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1593 IK8552339

Alarm	Attributes	Applicable major release
Name: IK8552339 (7262) Type: communicationsAlarm Package: Img.IK8552339 Raised on class: Img.FilePrepare	Severity: minor Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicRedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1594 IK8552341

Alarm	Attributes	Applicable major release
Name: IK8552341 (7263) Type: communicationsAlarm Package: Img.IK8552341 Raised on class: Img.FilePrepare	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1595 IK8552343

Alarm	Attributes	Applicable major release
Name: IK8552343 (7264) Type: communicationsAlarm Package: Img.IK8552343 Raised on class: Img.FilePrepare	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1596 IK8552344

Alarm	Attributes	Applicable major release
Name: IK8552344 (7265) Type: communicationsAlarm Package: lmg.IK8552344 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: like Activity Detected Trap Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: This alarm will be sent when the Virus Throttle Filter Driver detects virus like activity.\nAlarm to be cleared by the operator at the management system.\nReason: cpqNicVirusLikeActivityDetected		
Remedial action: The system reporting this trap requires immediate attention.		

Table 27-1597 IK8552347

Alarm	Attributes	Applicable major release
Name: IK8552347 (7266) Type: communicationsAlarm Package: lmg.IK8552347 Raised on class: lmg.FilePrepare	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1598 IK8552349

Alarm	Attributes	Applicable major release
Name: IK8552349 (7267) Type: communicationsAlarm Package: lmg.IK8552349 Raised on class: lmg.FilePrepare	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-1599 IK8552360

Alarm	Attributes	Applicable major release
Name: IK8552360 (7268) Type: equipmentAlarm Package: Img.IK8552360 Raised on class: Img.FilePrepare	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-1600 IK8552361

Alarm	Attributes	Applicable major release
Name: IK8552361 (7269) Type: equipmentAlarm Package: Img.IK8552361 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Enclosure temperature degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to degraded. This alarm signifies that an enclosure temperature sensor has been tripped indicating a possible overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempDegraded		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-1601 IK8552363

Alarm	Attributes	Applicable major release
Name: IK8552363 (7270) Type: environmentalAlarm Package: Img.IK8552363 Raised on class: Img.FilePrepare	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-1602 IK8552364

Alarm	Attributes	Applicable major release
Name: IK8552364 (7271) Type: environmentalAlarm Package: lmg.IK8552364 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to degraded. This alarm signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-1603 IK8552368

Alarm	Attributes	Applicable major release
Name: IK8552368 (7272) Type: equipmentAlarm Package: lmg.IK8552368 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1604 IK8552369

Alarm	Attributes	Applicable major release
Name: IK8552369 (7273) Type: equipmentAlarm Package: lmg.IK8552369 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-1605 IK8552373

Alarm	Attributes	Applicable major release
Name: IK8552373 (7274) Type: equipmentAlarm Package: Img.IK8552373 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem is no longer in a redundant state.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemNotRedundant		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-1606 IK8552374

Alarm	Attributes	Applicable major release
Name: IK8552374 (7275) Type: equipmentAlarm Package: Img.IK8552374 Raised on class: Img.FilePrepare	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-1607 IK8552375

Alarm	Attributes	Applicable major release
Name: IK8552375 (7276) Type: equipmentAlarm Package: Img.IK8552375 Raised on class: Img.FilePrepare	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-1608 IK8552376

Alarm	Attributes	Applicable major release
Name: IK8552376 (7277) Type: equipmentAlarm Package: Img.IK8552376 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-1609 IK8552377

Alarm	Attributes	Applicable major release
Name: IK8552377 (7278) Type: equipmentAlarm Package: Img.IK8552377 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-1610 IK8552378

Alarm	Attributes	Applicable major release
Name: IK8552378 (7279) Type: equipmentAlarm Package: Img.IK8552378 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-1611 IK8552379

Alarm	Attributes	Applicable major release
Name: IK8552379 (7280) Type: equipmentAlarm Package: Img.IK8552379 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-1612 IK8552380

Alarm	Attributes	Applicable major release
Name: IK8552380 (7281) Type: equipmentAlarm Package: Img.IK8552380 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedPowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-1613 IK8552382

Alarm	Attributes	Applicable major release
Name: IK8552382 (7282) Type: environmentalAlarm Package: Img.IK8552382 Raised on class: Img.FilePrepare	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-1614 IK8552385

Alarm	Attributes	Applicable major release
Name: IK8552385 (7283) Type: equipmentAlarm Package: lmg.IK8552385 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisNotLoadBalanced		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies. Add additional power supplies if needed.		

Table 27-1615 IK8552386

Alarm	Attributes	Applicable major release
Name: IK8552386 (7284) Type: equipmentAlarm Package: lmg.IK8552386 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1616 IK8552387

Alarm	Attributes	Applicable major release
Name: IK8552387 (7285) Type: equipmentAlarm Package: lmg.IK8552387 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1617 IK8552388

Alarm	Attributes	Applicable major release
Name: IK8552388 (7286) Type: equipmentAlarm Package: Img.IK8552388 Raised on class: Img.FilePrepare	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-1618 IK8552389

Alarm	Attributes	Applicable major release
Name: IK8552389 (7287) Type: equipmentAlarm Package: Img.IK8552389 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisLoadBalancingWireMissing		
Remedial action: Connect the load balancing wire.		

Table 27-1619 IK8552390

Alarm	Attributes	Applicable major release
Name: IK8552390 (7288) Type: equipmentAlarm Package: Img.IK8552390 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisTooManyPowerChassis		
Remedial action: Remove the extra power enclosure.		

Table 27-1620 IK8552391

Alarm	Attributes	Applicable major release
Name: IK8552391 (7289) Type: processingErrorAlarm Package: lmg.IK8552391 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-1621 IK8552392

Alarm	Attributes	Applicable major release
Name: IK8552392 (7290) Type: qualityOfServiceAlarm Package: lmg.IK8552392 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Enclosure manager degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The Onboard Administrator or other management processor status has been set to degraded. This alarm signifies that either an Onboard Administrator has failed but the other Onboard Administrator is still operating, or one or more management processors is in a non-optimal operating state.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureManagerDegraded		
Remedial action: For C-Class enclosures, replace the Onboard Administrator as soon as possible. For all others please refer to product documenation for possible corrective actions		

Table 27-1622 IK8552397

Alarm	Attributes	Applicable major release
Name: IK8552397 (7291) Type: communicationsAlarm Package: lmg.IK8552397 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: keying failed Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The server blade e-keying has failed. This alarm signifies that a server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackServerBladeEKeyingFailed		
Remedial action: Reconfigure server blade mezz cards.		

Table 27-1623 IK8552401

Alarm	Attributes	Applicable major release
Name: IK8552401 (7292) Type: communicationsAlarm Package: lmg.IK8552401 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-1624 IK8552402

Alarm	Attributes	Applicable major release
Name: IK8552402 (7293) Type: communicationsAlarm Package: lmg.IK8552402 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Interconnect degraded Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The interconnect status has been set to degraded. This alarm signifies that a interconnect has degraded.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorDegraded		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-1625 IK8552408

Alarm	Attributes	Applicable major release
Name: IK8552408 (7294) Type: qualityOfServiceAlarm Package: lmg.IK8552408 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1626 IK8552409

Alarm	Attributes	Applicable major release
Name: IK8552409 (7295) Type: processingErrorAlarm Package: lmg.IK8552409 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1627 IK8552410

Alarm	Attributes	Applicable major release
Name: IK8552410 (7296) Type: equipmentAlarm Package: lmg.IK8552410 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeGrpCapTimeout		
Remedial action: Reset the iLO management processor.		

Table 27-1628 IK8552411

Alarm	Attributes	Applicable major release
Name: IK8552411 (7297) Type: equipmentAlarm Package: lmg.IK8552411 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-1629 IK8552427

Alarm	Attributes	Applicable major release
Name: IK8552427 (7298) Type: equipmentAlarm Package: lmg.IK8552427 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: Generic EAE Minor trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Minor trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMinorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1630 IK8552428

Alarm	Attributes	Applicable major release
Name: IK8552428 (7299) Type: equipmentAlarm Package: lmg.IK8552428 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1631 IK8552429

Alarm	Attributes	Applicable major release
Name: IK8552429 (7300) Type: equipmentAlarm Package: lmg.IK8552429 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1632 IK8552430

Alarm	Attributes	Applicable major release
Name: IK8552430 (7301) Type: equipmentAlarm Package: lmg.IK8552430 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMinorEAETrap		

Table 27-1632 IK8552430 (continued)

Alarm	Attributes	Applicable major release
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1633 IK8552431

Alarm	Attributes	Applicable major release
Name: IK8552431 (7302) Type: equipmentAlarm Package: lmg.IK8552431 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1634 IK8552432

Alarm	Attributes	Applicable major release
Name: IK8552432 (7303) Type: equipmentAlarm Package: lmg.IK8552432 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-1635 IK8552435

Alarm	Attributes	Applicable major release
Name: IK8552435 (7304) Type: equipmentAlarm Package: lmg.IK8552435 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: Generic WSMAN Minor trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Minor trap\nReason: cpqRackMinorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1636 IK8552436

Alarm	Attributes	Applicable major release
Name: IK8552436 (7305) Type: equipmentAlarm Package: lmg.IK8552436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1637 IK8552437

Alarm	Attributes	Applicable major release
Name: IK8552437 (7306) Type: equipmentAlarm Package: lmg.IK8552437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1638 IK8552439

Alarm	Attributes	Applicable major release
Name: IK8552439 (7307) Type: communicationsAlarm Package: lmg.IK8552439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1639 IK8552443

Alarm	Attributes	Applicable major release
Name: IK8552443 (7308) Type: communicationsAlarm Package: lmg.IK8552443 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapDeviceConnected		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-1640 IK8552444

Alarm	Attributes	Applicable major release
Name: IK8552444 (7309) Type: communicationsAlarm Package: lmg.IK8552444 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapConnectionLost		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-1641 IK8552449

Alarm	Attributes	Applicable major release
Name: IK8552449 (7310) Type: environmentalAlarm Package: lmg.IK8552449 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 1 Above Warning Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 1 above warning threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp1AboveWarn		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1642 IK8552450

Alarm	Attributes	Applicable major release
Name: IK8552450 (7311) Type: environmentalAlarm Package: lmg.IK8552450 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 1 Above Maximum Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 1 above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp1AboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1643 IK8552453

Alarm	Attributes	Applicable major release
Name: IK8552453 (7312) Type: environmentalAlarm Package: lmg.IK8552453 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 2 Above Warning Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 2 above warning threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp2AboveWarn		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1644 IK8552454

Alarm	Attributes	Applicable major release
Name: IK8552454 (7313) Type: environmentalAlarm Package: lmg.IK8552454 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 2 Above Maximum Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 2 above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp2AboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1645 IK8552457

Alarm	Attributes	Applicable major release
Name: IK8552457 (7314) Type: equipmentAlarm Package: Img.IK8552457 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A CMC device is reporting voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCVoltOver		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1646 IK8552460

Alarm	Attributes	Applicable major release
Name: IK8552460 (7315) Type: environmentalAlarm Package: Img.IK8552460 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Humidity Above Maximum Implicitly cleared: false Default probable cause: humidityUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting humidity above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCHmdtOver		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1647 IK8552462

Alarm	Attributes	Applicable major release
Name: IK8552462 (7316) Type: environmentalAlarm Package: Img.IK8552462 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-1648 IK8552464

Alarm	Attributes	Applicable major release
Name: IK8552464 (7317) Type: equipmentAlarm Package: Img.IK8552464 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1648 IK8552464 (continued)

Alarm	Attributes	Applicable major release
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1649 IK8552466

Alarm	Attributes	Applicable major release
Name: IK8552466 (7318) Type: equipmentAlarm Package: Img.IK8552466 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Aux 1 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A CMC device has entered an alarm condition for auxiliary input 1.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux1Alarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1650 IK8552468

Alarm	Attributes	Applicable major release
Name: IK8552468 (7319) Type: equipmentAlarm Package: Img.IK8552468 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1651 IK8552489

Alarm	Attributes	Applicable major release
Name: IK8552489 (7320) Type: equipmentAlarm Package: Img.IK8552489 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: UPS Input Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A UPS device is reporting input voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSInputVoltageAboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1652 IK8552490

Alarm	Attributes	Applicable major release
Name: IK8552490 (7321) Type: equipmentAlarm Package: Img.IK8552490 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSInputVoltageNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-1653 IK8552492

Alarm	Attributes	Applicable major release
Name: IK8552492 (7322) Type: equipmentAlarm Package: Img.IK8552492 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: UPS Output Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A UPS device is reporting output voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSOutputVoltageAboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1654 IK8552493

Alarm	Attributes	Applicable major release
Name: IK8552493 (7323) Type: equipmentAlarm Package: Img.IK8552493 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOutputVoltageNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-1655 IK8552494

Alarm	Attributes	Applicable major release
Name: IK8552494 (7324) Type: equipmentAlarm Package: Img.IK8552494 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutputOverload		
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-1656 IK8552496

Alarm	Attributes	Applicable major release
Name: IK8552496 (7325) Type: environmentalAlarm Package: Img.IK8552496 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-1657 IK8552499

Alarm	Attributes	Applicable major release
Name: IK8552499 (7326) Type: equipmentAlarm Package: Img.IK8552499 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSBatteryLevelNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-1658 IK8552500

Alarm	Attributes	Applicable major release
Name: IK8552500 (7327) Type: equipmentAlarm Package: Img.IK8552500 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-1659 IK8552502

Alarm	Attributes	Applicable major release
Name: IK8552502 (7328) Type: equipmentAlarm Package: Img.IK8552502 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBuck		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-1660 IK8552503

Alarm	Attributes	Applicable major release
Name: IK8552503 (7329) Type: equipmentAlarm Package: Img.IK8552503 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBoost		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-1661 IK8552504

Alarm	Attributes	Applicable major release
Name: IK8552504 (7330) Type: equipmentAlarm Package: Img.IK8552504 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-1661 IK8552504 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnUtilityPower		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-1662 IK8552506

Alarm	Attributes	Applicable major release
Name: IK8552506 (7331) Type: environmentalAlarm Package: lmg.IK8552506 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: UPS Temperature High Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A UPS device is reporting temperature above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSTemperatureHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1663 IK8552507

Alarm	Attributes	Applicable major release
Name: IK8552507 (7332) Type: environmentalAlarm Package: lmg.IK8552507 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSTemperatureNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-1664 IK8552508

Alarm	Attributes	Applicable major release
Name: IK8552508 (7333) Type: equipmentAlarm Package: lmg.IK8552508 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		

Table 27-1664 IK8552508 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1665 IK8552510

Alarm	Attributes	Applicable major release
Name: IK8552510 (7334) Type: environmentalAlarm Package: lmg.IK8552510 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-1666 IK8552512

Alarm	Attributes	Applicable major release
Name: IK8552512 (7335) Type: equipmentAlarm Package: lmg.IK8552512 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestFailed		
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-1667 IK8552513

Alarm	Attributes	Applicable major release
Name: IK8552513 (7336) Type: equipmentAlarm Package: lmg.IK8552513 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestSucceeded		
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-1668 IK8552516

Alarm	Attributes	Applicable major release
Name: IK8552516 (7337) Type: equipmentAlarm Package: Img.IK8552516 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: DC Start Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The UPS has been started on battery when AC input power is not present. This alarm is used to record the date and time of this event.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSDCStartOccurred		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1669 IK8552518

Alarm	Attributes	Applicable major release
Name: IK8552518 (7338) Type: equipmentAlarm Package: Img.IK8552518 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1670 IK8552522

Alarm	Attributes	Applicable major release
Name: IK8552522 (7339) Type: equipmentAlarm Package: Img.IK8552522 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Utility Not Present Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Indicates that the utility input is not present. This differs from alarm #57 in that the detected voltage is zero in this case.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSUtilityNotPresent		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1671 IK8552526

Alarm	Attributes	Applicable major release
Name: IK8552526 (7340) Type: equipmentAlarm Package: Img.IK8552526 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringFault		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-1672 IK8552527

Alarm	Attributes	Applicable major release
Name: IK8552527 (7341) Type: equipmentAlarm Package: Img.IK8552527 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-1673 IK8552528

Alarm	Attributes	Applicable major release
Name: IK8552528 (7342) Type: equipmentAlarm Package: Img.IK8552528 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassOffManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-1674 IK8552529

Alarm	Attributes	Applicable major release
Name: IK8552529 (7343) Type: equipmentAlarm Package: Img.IK8552529 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassONManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-1675 IK8552531

Alarm	Attributes	Applicable major release
Name: IK8552531 (7344) Type: equipmentAlarm Package: Img.IK8552531 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-1676 IK8552533

Alarm	Attributes	Applicable major release
Name: IK8552533 (7345) Type: equipmentAlarm Package: Img.IK8552533 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInput-OutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-1677 IK8552534

Alarm	Attributes	Applicable major release
Name: IK8552534 (7346) Type: environmentalAlarm Package: lmg.IK8552534 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTemperatureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-1678 IK8552536

Alarm	Attributes	Applicable major release
Name: IK8552536 (7347) Type: equipmentAlarm Package: lmg.IK8552536 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassOnAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-1679 IK8552538

Alarm	Attributes	Applicable major release
Name: IK8552538 (7348) Type: equipmentAlarm Package: lmg.IK8552538 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMtrapUPSOutputoutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-1680 IK8552539

Alarm	Attributes	Applicable major release
Name: IK8552539 (7349) Type: equipmentAlarm Package: lmg.IK8552539 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-1681 IK8552541

Alarm	Attributes	Applicable major release
Name: IK8552541 (7350) Type: environmentalAlarm Package: lmg.IK8552541 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-1682 IK8552543

Alarm	Attributes	Applicable major release
Name: IK8552543 (7351) Type: equipmentAlarm Package: lmg.IK8552543 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1683 IK8552545

Alarm	Attributes	Applicable major release
Name: IK8552545 (7352) Type: equipmentAlarm Package: lmg.IK8552545 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSEPOInitiated		
Remedial action: Perform the following steps to clear the alarm: 1. Turn the UPS on to reapply power to attached equipment.		

Table 27-1684 IK8552546

Alarm	Attributes	Applicable major release
Name: IK8552546 (9283) Type: equipmentAlarm Package: lmg.IK8552546 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1685 IK8552548

Alarm	Attributes	Applicable major release
Name: IK8552548 (7353) Type: environmentalAlarm Package: lmg.IK8552548 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If the problem persists, contact NOKIA customer support.		

Table 27-1686 IK8552550

Alarm	Attributes	Applicable major release
Name: IK8552550 (7354) Type: environmentalAlarm Package: Img.IK8552550 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If the problem persists, contact NOKIA customer support.		

Table 27-1687 IK8552552

Alarm	Attributes	Applicable major release
Name: IK8552552 (7355) Type: processingErrorAlarm Package: Img.IK8552552 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-1688 IK8552554

Alarm	Attributes	Applicable major release
Name: IK8552554 (7356) Type: equipmentAlarm Package: Img.IK8552554 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-1689 IK8552556

Alarm	Attributes	Applicable major release
Name: IK8552556 (7357) Type: equipmentAlarm Package: Img.IK8552556 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-1690 IK8552559

Alarm	Attributes	Applicable major release
Name: IK8552559 (7358) Type: equipmentAlarm Package: Img.IK8552559 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-1691 IK8552560

Alarm	Attributes	Applicable major release
Name: IK8552560 (7359) Type: equipmentAlarm Package: Img.IK8552560 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A warning alarm has occurred.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqPMTrapWarning		
Remedial action: Check the Trap Details for more information.		

Table 27-1692 IK8552585

Alarm	Attributes	Applicable major release
Name: IK8552585 (7360) Type: processingErrorAlarm Package: Img.IK8552585 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-1693 IK8552586

Alarm	Attributes	Applicable major release
Name: IK8552586 (7361) Type: equipmentAlarm Package: Img.IK8552586 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-1694 IK8552590

Alarm	Attributes	Applicable major release
Name: IK8552590 (7362) Type: environmentalAlarm Package: Img.IK8552590 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3LibraryDoorOpen		
Remedial action: Close the door on the tape library.		

Table 27-1695 IK8552606

Alarm	Attributes	Applicable major release
Name: IK8552606 (7363) Type: equipmentAlarm Package: lmg.IK8552606 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHoodRemoved		
Remedial action: Replace the cover (hood), ensure the system's cover is properly installed. Verify the system is in working order.		

Table 27-1696 IK8552608

Alarm	Attributes	Applicable major release
Name: IK8552608 (7364) Type: environmentalAlarm Package: lmg.IK8552608 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Monitor Condition Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits for the monitor indicated by the cpqSiMonitorIndex. The monitor's condition is degraded due to the internal temperature exceeding normal operating limits. The monitor is still useable, but action should be taken to return the condition to OK.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionDegraded		
Remedial action: Physically check for obstructions to air flow around the monitor. Check the thermostat in the room that the system occupies. Allow the monitor to cool by turning off the monitor for 5 minutes then turn the monitor back on. After the monitor cools, another alarm indicating an improving condition, such as Monitor OK, will be issued.		

Table 27-1697 IK8552609

Alarm	Attributes	Applicable major release
Name: IK8552609 (7365) Type: processingErrorAlarm Package: lmg.IK8552609 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1698 IK8552610

Alarm	Attributes	Applicable major release
Name: IK8552610 (7366) Type: processingErrorAlarm Package: Img.IK8552610 Raised on class: Img.FilePrepare	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-1699 IK8552612

Alarm	Attributes	Applicable major release
Name: IK8552612 (7367) Type: processingErrorAlarm Package: Img.IK8552612 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiMemConfigChange		
Remedial action: You may want to verify a valid reason for a memory configuration to have occurred. If system issuing the alert is a Desktop running NT, the memory configuration change information is also logged in the NT System Log.		

Table 27-1700 IK8552615

Alarm	Attributes	Applicable major release
Name: IK8552615 (7368) Type: equipmentAlarm Package: Img.IK8552615 Raised on class: Img.FilePrepare	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-1701 IK8552616

Alarm	Attributes	Applicable major release
Name: IK8552616 (7369) Type: environmentalAlarm Package: Img.IK8552616 Raised on class: Img.FilePrepare	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-1702 IK8552617

Alarm	Attributes	Applicable major release
Name: IK8552617 (7370) Type: environmentalAlarm Package: Img.IK8552617 Raised on class: Img.FilePrepare	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-1703 IK8552618

Alarm	Attributes	Applicable major release
Name: IK8552618 (7371) Type: environmentalAlarm Package: Img.IK8552618 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryCalibrationError		
Remedial action: Run the Power Conservation Utility. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-1704 IK8552619

Alarm	Attributes	Applicable major release
Name: IK8552619 (7372) Type: processingErrorAlarm Package: Img.IK8552619 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Server Reset Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Reset Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server reset.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerReset		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1705 IK8552620

Alarm	Attributes	Applicable major release
Name: IK8552620 (7373) Type: equipmentAlarm Package: Img.IK8552620 Raised on class: Img.FilePrepare	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-1706 IK8552621

Alarm	Attributes	Applicable major release
Name: IK8552621 (7374) Type: securityServiceOrMechanismViolation Package: Img.IK8552621 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Out Unauthorized Login Attempts Implicitly cleared: false Default probable cause: unauthorizedAccessAttempt	Release: • LR14.3.MG
Description: Remote Insight/ Integrated Lights-Out Unauthorized Login Attempts. The Remote Insight/ Integrated Lights-Out firmware has detected unauthorized login attempts.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2UnauthorizedLoginAttempts		
Remedial action: Check the iLO log for more information on the login failure.		

Table 27-1707 IK8552622

Alarm	Attributes	Applicable major release
Name: IK8552622 (7375) Type: environmentalAlarm Package: Img.IK8552622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG

Table 27-1707 IK8552622 (continued)

Alarm	Attributes	Applicable major release
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-1708 IK8552628

Alarm	Attributes	Applicable major release
Name: IK8552628 (7376) Type: equipmentAlarm Package: lmg.IK8552628 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-1709 IK8552630

Alarm	Attributes	Applicable major release
Name: IK8552630 (7377) Type: processingErrorAlarm Package: lmg.IK8552630 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Security override engaged Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Security Override Engaged. The Remote Insight/ Integrated Lights-Out firmware has detected the security override jumper has been toggled to the engaged position.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2SecurityOverrideEngaged		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1710 IK8552631

Alarm	Attributes	Applicable major release
Name: IK8552631 (7378) Type: processingErrorAlarm Package: lmg.IK8552631 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Security override disengaged Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Security Override Disengaged. The Remote Insight/ Integrated Lights-Out firmware has detected the security override jumper has been toggled to the disengaged position.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2SecurityOverrideDisengaged		

Table 27-1710 IK8552631 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1711 IK8552632

Alarm	Attributes	Applicable major release
Name: IK8552632 (7379) Type: processingErrorAlarm Package: Img.IK8552632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1712 IK8552633

Alarm	Attributes	Applicable major release
Name: IK8552633 (7380) Type: communicationsAlarm Package: Img.IK8552633 Raised on class: Img.FilePrepare	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-1713 IK8552636

Alarm	Attributes	Applicable major release
Name: IK8552636 (9284) Type: equipmentAlarm Package: Img.IK8552636 Raised on class: Img.FilePrepare	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1714 IK8552647

Alarm	Attributes	Applicable major release
Name: IK8552647 (7381) Type: qualityOfServiceAlarm Package: lmg.IK8552647 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: PC Card Thermal Degraded Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for safe operations thereby causing degraded operations. This alarm will be sent when cpqSePCCardStatus transitions from Normal (1) to Thermal Degraded (2). The manufacturer and product information strings as well as the slot number for the degraded PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalDegraded		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1715 IK8552648

Alarm	Attributes	Applicable major release
Name: IK8552648 (7382) Type: qualityOfServiceAlarm Package: lmg.IK8552648 Raised on class: lmg.FilePrepare	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1716 IK8552657

Alarm	Attributes	Applicable major release
Name: IK8552657 (7383) Type: environmentalAlarm Package: lmg.IK8552657 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1717 IK8552658

Alarm	Attributes	Applicable major release
Name: IK8552658 (7384) Type: environmentalAlarm Package: lmg.IK8552658 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system.\nReason: cpqSsTempDegraded		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1718 IK8552661

Alarm	Attributes	Applicable major release
Name: IK8552661 (7385) Type: equipmentAlarm Package: lmg.IK8552661 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system.\nReason: cpqSsSidePanelRemoved		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1719 IK8552662

Alarm	Attributes	Applicable major release
Name: IK8552662 (7386) Type: equipmentAlarm Package: lmg.IK8552662 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A storage system power supply status has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSsPwrSupplyDegraded		
Remedial action: check the storage system power supply		

Table 27-1720 IK8552664

Alarm	Attributes	Applicable major release
Name: IK8552664 (7387) Type: environmentalAlarm Package: lmg.IK8552664 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempFailed		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-1721 IK8552665

Alarm	Attributes	Applicable major release
Name: IK8552665 (7388) Type: environmentalAlarm Package: lmg.IK8552665 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempDegraded		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-1722 IK8552668

Alarm	Attributes	Applicable major release
Name: IK8552668 (7389) Type: equipmentAlarm Package: lmg.IK8552668 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3SidePanelRemoved		
Remedial action: Replace the storage system side panel.		

Table 27-1723 IK8552669

Alarm	Attributes	Applicable major release
Name: IK8552669 (7390) Type: equipmentAlarm Package: Img.IK8552669 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A storage system power supply status has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSs3PwrSupplyDegraded		
Remedial action: check the storage system power supply		

Table 27-1724 IK8552670

Alarm	Attributes	Applicable major release
Name: IK8552670 (7391) Type: equipmentAlarm Package: Img.IK8552670 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A storage system power supply status has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs4PwrSupplyDegraded		
Remedial action: Take action to restore power or replace any failed storage system power supply.		

Table 27-1725 IK8552695

Alarm	Attributes	Applicable major release
Name: IK8552695 (7392) Type: equipmentAlarm Package: Img.IK8552695 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMeRisingAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1726 IK8552697

Alarm	Attributes	Applicable major release
Name: IK8552697 (7393) Type: equipmentAlarm Package: Img.IK8552697 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-1726 IK8552697 (continued)

Alarm	Attributes	Applicable major release
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMe2RisingAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1727 IK8552699

Alarm	Attributes	Applicable major release
Name: IK8552699 (7394) Type: equipmentAlarm Package: lmg.IK8552699 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMeRisingAlarm-Extended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1728 IK8552700

Alarm	Attributes	Applicable major release
Name: IK8552700 (7395) Type: equipmentAlarm Package: lmg.IK8552700 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Falling Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Falling Threshold passed. An alarm entry has crossed its falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeFallingAlarmExtended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1729 IK8552701

Alarm	Attributes	Applicable major release
Name: IK8552701 (7396) Type: equipmentAlarm Package: lmg.IK8552701 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Critical Rising Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Critical Rising Threshold passed. An alarm entry has crossed its Critical rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeCriticalRisingAlarmExtended		

Table 27-1729 IK8552701 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1730 IK8552702

Alarm	Attributes	Applicable major release
Name: IK8552702 (7397) Type: equipmentAlarm Package: lmg.IK8552702 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: Critical Falling Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Critical Falling Threshold passed. An alarm entry has crossed its Critical falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeCriticalFallingAlarmExtended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1731 IK8552748

Alarm	Attributes	Applicable major release
Name: IK8552748 (7398) Type: equipmentAlarm Package: lmg.IK8552748 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: fluteModuleAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Alarm notification\nAlarm is cleared by the system.\nReason: fluteModuleAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1732 IK8554762

Alarm	Attributes	Applicable major release
Name: IK8554762 (7399) Type: communicationsAlarm Package: lmg.IK8554762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1733 IK8557456

Alarm	Attributes	Applicable major release
Name: IK8557456 (9285) Type: environmentalAlarm Package: Img.IK8557456 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The temperature at rack sensor 1 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp1		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1734 IK8557457

Alarm	Attributes	Applicable major release
Name: IK8557457 (9286) Type: environmentalAlarm Package: Img.IK8557457 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The temperature at rack sensor 2 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp2		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1735 IK8557458

Alarm	Attributes	Applicable major release
Name: IK8557458 (9287) Type: environmentalAlarm Package: Img.IK8557458 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The status of Fan 1 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan1		
Remedial action: Refer to Trap Details for more information.		

Table 27-1736 IK8557459

Alarm	Attributes	Applicable major release
Name: IK8557459 (9288) Type: environmentalAlarm Package: Img.IK8557459 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG

Table 27-1736 IK8557459 (continued)

Alarm	Attributes	Applicable major release
Description: The status of Fan 2 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan2		
Remedial action: Refer to Trap Details for more information.		

Table 27-1737 IK8557460

Alarm	Attributes	Applicable major release
Name: IK8557460 (9289) Type: equipmentAlarm Package: Img.IK8557460 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Voltage-alarm Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The AC voltage of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmVoltage		
Remedial action: Check the incoming power source and ensure all cables are inserted correctly.		

Table 27-1738 IK8557461

Alarm	Attributes	Applicable major release
Name: IK8557461 (9290) Type: environmentalAlarm Package: Img.IK8557461 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Humidity-alarm Implicitly cleared: true Default probable cause: humidityUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The humidity of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmHumidity		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-1739 IK8557462

Alarm	Attributes	Applicable major release
Name: IK8557462 (9291) Type: environmentalAlarm Package: Img.IK8557462 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #1).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput1		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1740 IK8557463

Alarm	Attributes	Applicable major release
Name: IK8557463 (9292) Type: environmentalAlarm Package: lmg.IK8557463 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #2).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput2		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1741 IK8557464

Alarm	Attributes	Applicable major release
Name: IK8557464 (9293) Type: environmentalAlarm Package: lmg.IK8557464 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #3).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput3		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1742 IK8557465

Alarm	Attributes	Applicable major release
Name: IK8557465 (9294) Type: environmentalAlarm Package: lmg.IK8557465 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #4).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput4		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1743 IK8557466

Alarm	Attributes	Applicable major release
Name: IK8557466 (9295) Type: processingErrorAlarm Package: lmg.IK8557466 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG

Table 27-1743 IK8557466 (continued)

Alarm	Attributes	Applicable major release
Description: Rack door lock #1 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1744 IK8557467

Alarm	Attributes	Applicable major release
Name: IK8557467 (9296) Type: processingErrorAlarm Package: Img.IK8557467 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: Rack door lock #2 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-1745 IK8557468

Alarm	Attributes	Applicable major release
Name: IK8557468 (9297) Type: environmentalAlarm Package: Img.IK8557468 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Smoke-alarm Implicitly cleared: true Default probable cause: smoke	Release: • LR15.1.MG • LR16.1.MG
Description: The rack smoke detector has detected smoke.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmSmoke		
Remedial action: Investigate rack for an over temperature condition and refer to Trap Details for more information.		

Table 27-1746 IK8557469

Alarm	Attributes	Applicable major release
Name: IK8557469 (9298) Type: environmentalAlarm Package: Img.IK8557469 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Shock-alarm Implicitly cleared: true Default probable cause: excessiveVibration	Release: • LR15.1.MG • LR16.1.MG
Description: The rack shock detector has detected a vibration to the rack.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmShock		
Remedial action: Investigate rack.		

Table 27-1747 IK8557474

Alarm	Attributes	Applicable major release
Name: IK8557474 (9299) Type: processingErrorAlarm Package: lmg.IK8557474 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: The rack door locking device #1 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-1748 IK8557475

Alarm	Attributes	Applicable major release
Name: IK8557475 (9300) Type: processingErrorAlarm Package: lmg.IK8557475 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: The rack door locking device #2 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-1749 IK8557477

Alarm	Attributes	Applicable major release
Name: IK8557477 (9301) Type: processingErrorAlarm Package: lmg.IK8557477 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Corrected - uncorrectable Memory Errors - Replace Memory Module Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG • LR16.1.MG
Description: Corrected - uncorrected Memory Errors Detected The errors have been corrected, but the memory module should be replaced. Value 0 for CPU means memory is not Processor based\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqHe5CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module.		

Table 27-1750 IK8557478

Alarm	Attributes	Applicable major release
Name: IK8557478 (9302) Type: communicationsAlarm Package: lmg.IK8557478 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: NIC Virus-like Activity Detected Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent when the Virus Throttle Filter Driver detects virus like activity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNicVirusLikeActivityDetected		
Remedial action: The system reporting this trap requires immediate attention.		

Table 27-1751 IK8557479

Alarm	Attributes	Applicable major release
Name: IK8557479 (9303) Type: communicationsAlarm Package: lmg.IK8557479 Raised on class: lmg.FilePrepare	Severity: minor Specific problem: Server Blade e-keying failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: The server blade e-keying has failed. This alarm signifies that a server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeEKeyingFailed		
Remedial action: Reconfigure server blade mezz cards.		

Table 27-1752 IK8557481

Alarm	Attributes	Applicable major release
Name: IK8557481 (10612) Type: processingErrorAlarm Package: lmg.IK8557481 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.		
Remedial action: No action is required.		

Table 27-1753 IK8557482

Alarm	Attributes	Applicable major release
Name: IK8557482 (10613) Type: processingErrorAlarm Package: Img.IK8557482 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.		
Remedial action: No action is required.		

Table 27-1754 IK8557483

Alarm	Attributes	Applicable major release
Name: IK8557483 (10614) Type: processingErrorAlarm Package: Img.IK8557483 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.		
Remedial action: No action is required.		

Table 27-1755 IK8557484

Alarm	Attributes	Applicable major release
Name: IK8557484 (10615) Type: processingErrorAlarm Package: Img.IK8557484 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.		
Remedial action: No action is required.		

Table 27-1756 IK8557485

Alarm	Attributes	Applicable major release
Name: IK8557485 (10616) Type: processingErrorAlarm Package: Img.IK8557485 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.		
Remedial action: No action is required.		

Table 27-1757 IK8557486

Alarm	Attributes	Applicable major release
Name: IK8557486 (10617) Type: processingErrorAlarm Package: Img.IK8557486 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-1758 IK8557487

Alarm	Attributes	Applicable major release
Name: IK8557487 (10618) Type: processingErrorAlarm Package: Img.IK8557487 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-1759 IK8557488

Alarm	Attributes	Applicable major release
Name: IK8557488 (10619) Type: processingErrorAlarm Package: Img.IK8557488 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-1760 IK8557489

Alarm	Attributes	Applicable major release
Name: IK8557489 (10620) Type: processingErrorAlarm Package: Img.IK8557489 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.		

Table 27-1760 IK8557489 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1761 IK8557490

Alarm	Attributes	Applicable major release
Name: IK8557490 (10621) Type: processingErrorAlarm Package: lmg.IK8557490 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-1762 IK8557491

Alarm	Attributes	Applicable major release
Name: IK8557491 (10622) Type: processingErrorAlarm Package: lmg.IK8557491 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-1763 IK8557500

Alarm	Attributes	Applicable major release
Name: IK8557500 (10623) Type: processingErrorAlarm Package: lmg.IK8557500 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes degraded.		
Remedial action: No action is required.		

Table 27-1764 IK8557501

Alarm	Attributes	Applicable major release
Name: IK8557501 (10624) Type: processingErrorAlarm Package: Img.IK8557501 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes failed.		
Remedial action: No action is required.		

Table 27-1765 IK8557502

Alarm	Attributes	Applicable major release
Name: IK8557502 (10625) Type: processingErrorAlarm Package: Img.IK8557502 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes degraded.		
Remedial action: No action is required.		

Table 27-1766 IK8557503

Alarm	Attributes	Applicable major release
Name: IK8557503 (10626) Type: processingErrorAlarm Package: Img.IK8557503 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes failed.		
Remedial action: No action is required.		

Table 27-1767 IK8557504

Alarm	Attributes	Applicable major release
Name: IK8557504 (10627) Type: processingErrorAlarm Package: Img.IK8557504 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes degraded.		

Table 27-1767 IK8557504 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1768 IK8557505

Alarm	Attributes	Applicable major release
Name: IK8557505 (10628) Type: processingErrorAlarm Package: lmg.IK8557505 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes failed.		
Remedial action: No action is required.		

Table 27-1769 IK8557508

Alarm	Attributes	Applicable major release
Name: IK8557508 (10629) Type: processingErrorAlarm Package: lmg.IK8557508 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1770 IK8557509

Alarm	Attributes	Applicable major release
Name: IK8557509 (10630) Type: processingErrorAlarm Package: lmg.IK8557509 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-1771 IK8557510

Alarm	Attributes	Applicable major release
Name: IK8557510 (10631) Type: processingErrorAlarm Package: Img.IK8557510 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: External Array Redundant Controller Active. This event signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.		
Remedial action: No action is required.		

Table 27-1772 IK8557511

Alarm	Attributes	Applicable major release
Name: IK8557511 (10632) Type: processingErrorAlarm Package: Img.IK8557511 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1773 IK8557512

Alarm	Attributes	Applicable major release
Name: IK8557512 (10633) Type: processingErrorAlarm Package: Img.IK8557512 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-1774 IK8557513

Alarm	Attributes	Applicable major release
Name: IK8557513 (10634) Type: processingErrorAlarm Package: Img.IK8557513 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log		
Remedial action: No action is required.		

Table 27-1775 IK8557514

Alarm	Attributes	Applicable major release
Name: IK8557514 (10635) Type: processingErrorAlarm Package: Img.IK8557514 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.		
Remedial action: No action is required.		

Table 27-1776 IK8557515

Alarm	Attributes	Applicable major release
Name: IK8557515 (10636) Type: processingErrorAlarm Package: Img.IK8557515 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-1777 IK8557516

Alarm	Attributes	Applicable major release
Name: IK8557516 (10637) Type: processingErrorAlarm Package: Img.IK8557516 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-1778 IK8557517

Alarm	Attributes	Applicable major release
Name: IK8557517 (10638) Type: processingErrorAlarm Package: Img.IK8557517 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-1779 IK8557518

Alarm	Attributes	Applicable major release
Name: IK8557518 (10639) Type: processingErrorAlarm Package: Img.IK8557518 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-1780 IK8557519

Alarm	Attributes	Applicable major release
Name: IK8557519 (10640) Type: processingErrorAlarm Package: Img.IK8557519 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.		
Remedial action: No action is required.		

Table 27-1781 IK8557520

Alarm	Attributes	Applicable major release
Name: IK8557520 (10641) Type: processingErrorAlarm Package: Img.IK8557520 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.		

Table 27-1781 IK8557520 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1782 IK8557521

Alarm	Attributes	Applicable major release
Name: IK8557521 (10642) Type: processingErrorAlarm Package: Img.IK8557521 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.		
Remedial action: No action is required.		

Table 27-1783 IK8557522

Alarm	Attributes	Applicable major release
Name: IK8557522 (10643) Type: processingErrorAlarm Package: Img.IK8557522 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.		
Remedial action: No action is required.		

Table 27-1784 IK8557523

Alarm	Attributes	Applicable major release
Name: IK8557523 (10644) Type: processingErrorAlarm Package: Img.IK8557523 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.		
Remedial action: No action is required.		

Table 27-1785 IK8557524

Alarm	Attributes	Applicable major release
Name: IK8557524 (10645) Type: processingErrorAlarm Package: Img.IK8557524 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.		
Remedial action: No action is required.		

Table 27-1786 IK8557525

Alarm	Attributes	Applicable major release
Name: IK8557525 (10646) Type: processingErrorAlarm Package: Img.IK8557525 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.		
Remedial action: No action is required.		

Table 27-1787 IK8557526

Alarm	Attributes	Applicable major release
Name: IK8557526 (10647) Type: processingErrorAlarm Package: Img.IK8557526 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.		
Remedial action: No action is required.		

Table 27-1788 IK8557527

Alarm	Attributes	Applicable major release
Name: IK8557527 (10648) Type: processingErrorAlarm Package: Img.IK8557527 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.		
Remedial action: No action is required.		

Table 27-1789 IK8557528

Alarm	Attributes	Applicable major release
Name: IK8557528 (10649) Type: processingErrorAlarm Package: Img.IK8557528 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-1790 IK8557529

Alarm	Attributes	Applicable major release
Name: IK8557529 (10650) Type: processingErrorAlarm Package: Img.IK8557529 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-1791 IK8557530

Alarm	Attributes	Applicable major release
Name: IK8557530 (10651) Type: processingErrorAlarm Package: Img.IK8557530 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.		
Remedial action: No action is required.		

Table 27-1792 IK8557531

Alarm	Attributes	Applicable major release
Name: IK8557531 (10652) Type: processingErrorAlarm Package: Img.IK8557531 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the configured redundant NIC becomes the active NIC.		
Remedial action: No action is required.		

Table 27-1793 IK8557532

Alarm	Attributes	Applicable major release
Name: IK8557532 (10653) Type: processingErrorAlarm Package: Img.IK8557532 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.MG
Description: This event is a send to the user to notify him of a Critical Software Update.		
Remedial action: No action is required.		

Table 27-1794 IK8557533

Alarm	Attributes	Applicable major release
Name: IK8557533 (10654) Type: processingErrorAlarm Package: Img.IK8557533 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-1794 IK8557533 (continued)

Alarm	Attributes	Applicable major release
Description: Controller Active. This event signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.		
Remedial action: No action is required.		

Table 27-1795 IK8557534

Alarm	Attributes	Applicable major release
Name: IK8557534 (10655) Type: processingErrorAlarm Package: lmg.IK8557534 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1796 IK8557535

Alarm	Attributes	Applicable major release
Name: IK8557535 (10656) Type: processingErrorAlarm Package: lmg.IK8557535 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Accelerator Board Bad Data. This event signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-1797 IK8557536

Alarm	Attributes	Applicable major release
Name: IK8557536 (10657) Type: processingErrorAlarm Package: lmg.IK8557536 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the array accelerator cache board.		
Remedial action: No action is required.		

Table 27-1798 IK8557537

Alarm	Attributes	Applicable major release
Name: IK8557537 (10658) Type: processingErrorAlarm Package: Img.IK8557537 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1799 IK8557538

Alarm	Attributes	Applicable major release
Name: IK8557538 (10659) Type: processingErrorAlarm Package: Img.IK8557538 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-1800 IK8557539

Alarm	Attributes	Applicable major release
Name: IK8557539 (10660) Type: processingErrorAlarm Package: Img.IK8557539 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Cache Module Board Bad Data. This event signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-1801 IK8557540

Alarm	Attributes	Applicable major release
Name: IK8557540 (10661) Type: processingErrorAlarm Package: Img.IK8557540 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG

Table 27-1801 IK8557540 (continued)

Alarm	Attributes	Applicable major release
Description: Cache Module Board Backup Power Source Failed. This event signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-1802 IK8557541

Alarm	Attributes	Applicable major release
Name: IK8557541 (10662) Type: processingErrorAlarm Package: Img.IK8557541 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-1803 IK8557542

Alarm	Attributes	Applicable major release
Name: IK8557542 (10663) Type: processingErrorAlarm Package: Img.IK8557542 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-1804 IK8557543

Alarm	Attributes	Applicable major release
Name: IK8557543 (10664) Type: processingErrorAlarm Package: Img.IK8557543 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.		
Remedial action: No action is required.		

Table 27-1805 IK8557545

Alarm	Attributes	Applicable major release
Name: IK8557545 (10665) Type: processingErrorAlarm Package: lmg.IK8557545 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.		
Remedial action: No action is required.		

Table 27-1806 IK8557546

Alarm	Attributes	Applicable major release
Name: IK8557546 (10666) Type: processingErrorAlarm Package: lmg.IK8557546 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to failed. This event signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-1807 IK8557547

Alarm	Attributes	Applicable major release
Name: IK8557547 (10667) Type: processingErrorAlarm Package: lmg.IK8557547 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to degraded. This event signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-1808 IK8557548

Alarm	Attributes	Applicable major release
Name: IK8557548 (10668) Type: processingErrorAlarm Package: Img.IK8557548 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to failed. This event signifies that a power supply has failed.		
Remedial action: No action is required.		

Table 27-1809 IK8557549

Alarm	Attributes	Applicable major release
Name: IK8557549 (10669) Type: processingErrorAlarm Package: Img.IK8557549 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to degraded. This event signifies that a power supply has degraded.		
Remedial action: No action is required.		

Table 27-1810 IK8557550

Alarm	Attributes	Applicable major release
Name: IK8557550 (10670) Type: processingErrorAlarm Package: Img.IK8557550 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem is no longer in a redundant state.		
Remedial action: No action is required.		

Table 27-1811 IK8557551

Alarm	Attributes	Applicable major release
Name: IK8557551 (10671) Type: processingErrorAlarm Package: Img.IK8557551 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power supply detected an input line voltage problem.		

Table 27-1811 IK8557551 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1812 IK8557552

Alarm	Attributes	Applicable major release
Name: IK8557552 (10672) Type: processingErrorAlarm Package: Img.IK8557552 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem overload condition.		
Remedial action: No action is required.		

Table 27-1813 IK8557553

Alarm	Attributes	Applicable major release
Name: IK8557553 (10673) Type: processingErrorAlarm Package: Img.IK8557553 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.		
Remedial action: No action is required.		

Table 27-1814 IK8557554

Alarm	Attributes	Applicable major release
Name: IK8557554 (10674) Type: processingErrorAlarm Package: Img.IK8557554 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.		
Remedial action: No action is required.		

Table 27-1815 IK8557555

Alarm	Attributes	Applicable major release
Name: IK8557555 (10675) Type: processingErrorAlarm Package: Img.IK8557555 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.		
Remedial action: No action is required.		

Table 27-1816 IK8557556

Alarm	Attributes	Applicable major release
Name: IK8557556 (10676) Type: processingErrorAlarm Package: Img.IK8557556 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-1817 IK8557557

Alarm	Attributes	Applicable major release
Name: IK8557557 (10677) Type: processingErrorAlarm Package: Img.IK8557557 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-1818 IK8557558

Alarm	Attributes	Applicable major release
Name: IK8557558 (10678) Type: processingErrorAlarm Package: Img.IK8557558 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Fuse open. The fuse has been tripped.		

Table 27-1818 IK8557558 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1819 IK8557559

Alarm	Attributes	Applicable major release
Name: IK8557559 (10679) Type: processingErrorAlarm Package: Img.IK8557559 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.		
Remedial action: No action is required.		

Table 27-1820 IK8557560

Alarm	Attributes	Applicable major release
Name: IK8557560 (10680) Type: processingErrorAlarm Package: Img.IK8557560 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.		
Remedial action: No action is required.		

Table 27-1821 IK8557561

Alarm	Attributes	Applicable major release
Name: IK8557561 (10681) Type: processingErrorAlarm Package: Img.IK8557561 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.		
Remedial action: No action is required.		

Table 27-1822 IK8557562

Alarm	Attributes	Applicable major release
Name: IK8557562 (10682) Type: processingErrorAlarm Package: lmg.IK8557562 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.		
Remedial action: No action is required.		

Table 27-1823 IK8557563

Alarm	Attributes	Applicable major release
Name: IK8557563 (10683) Type: processingErrorAlarm Package: lmg.IK8557563 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.		
Remedial action: No action is required.		

Table 27-1824 IK8557564

Alarm	Attributes	Applicable major release
Name: IK8557564 (10684) Type: processingErrorAlarm Package: lmg.IK8557564 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.		
Remedial action: No action is required.		

Table 27-1825 IK8557565

Alarm	Attributes	Applicable major release
Name: IK8557565 (10685) Type: processingErrorAlarm Package: lmg.IK8557565 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG

Table 27-1825 IK8557565 (continued)

Alarm	Attributes	Applicable major release
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.		
Remedial action: No action is required.		

Table 27-1826 IK8557566

Alarm	Attributes	Applicable major release
Name: IK8557566 (10686) Type: processingErrorAlarm Package: Img.IK8557566 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.		
Remedial action: No action is required.		

Table 27-1827 IK8557567

Alarm	Attributes	Applicable major release
Name: IK8557567 (10687) Type: processingErrorAlarm Package: Img.IK8557567 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper		
Remedial action: No action is required.		

Table 27-1828 IK8557568

Alarm	Attributes	Applicable major release
Name: IK8557568 (10688) Type: processingErrorAlarm Package: Img.IK8557568 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.		
Remedial action: No action is required.		

Table 27-1829 IK8557569

Alarm	Attributes	Applicable major release
Name: IK8557569 (10689) Type: processingErrorAlarm Package: Img.IK8557569 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.		
Remedial action: No action is required.		

Table 27-1830 IK8557570

Alarm	Attributes	Applicable major release
Name: IK8557570 (10690) Type: processingErrorAlarm Package: Img.IK8557570 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.		
Remedial action: No action is required.		

Table 27-1831 IK8557571

Alarm	Attributes	Applicable major release
Name: IK8557571 (10691) Type: processingErrorAlarm Package: Img.IK8557571 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.		
Remedial action: No action is required.		

Table 27-1832 IK8557572

Alarm	Attributes	Applicable major release
Name: IK8557572 (10692) Type: processingErrorAlarm Package: Img.IK8557572 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Generic WSMAN Major trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-1832 IK8557572 (continued)

Alarm	Attributes	Applicable major release
Description: WSMAN Major trap		
Remedial action: No action is required.		

Table 27-1833 IK8557573

Alarm	Attributes	Applicable major release
Name: IK8557573 (10693) Type: processingErrorAlarm Package: Img.IK8557573 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Generic WSMAN Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Critical trap		
Remedial action: No action is required.		

Table 27-1834 IK8557574

Alarm	Attributes	Applicable major release
Name: IK8557574 (10694) Type: processingErrorAlarm Package: Img.IK8557574 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-1835 IK8557575

Alarm	Attributes	Applicable major release
Name: IK8557575 (10695) Type: processingErrorAlarm Package: Img.IK8557575 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-1836 IK8557576

Alarm	Attributes	Applicable major release
Name: IK8557576 (10696) Type: processingErrorAlarm Package: Img.IK8557576 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.		
Remedial action: No action is required.		

Table 27-1837 IK8557577

Alarm	Attributes	Applicable major release
Name: IK8557577 (10697) Type: processingErrorAlarm Package: Img.IK8557577 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-1838 IK8557578

Alarm	Attributes	Applicable major release
Name: IK8557578 (10698) Type: processingErrorAlarm Package: Img.IK8557578 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.		
Remedial action: No action is required.		

Table 27-1839 IK8557579

Alarm	Attributes	Applicable major release
Name: IK8557579 (10699) Type: processingErrorAlarm Package: Img.IK8557579 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-1840 IK8557580

Alarm	Attributes	Applicable major release
Name: IK8557580 (10700) Type: processingErrorAlarm Package: Img.IK8557580 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.		
Remedial action: No action is required.		

Table 27-1841 IK8557581

Alarm	Attributes	Applicable major release
Name: IK8557581 (10701) Type: processingErrorAlarm Package: Img.IK8557581 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.		
Remedial action: No action is required.		

Table 27-1842 IK8557582

Alarm	Attributes	Applicable major release
Name: IK8557582 (10702) Type: processingErrorAlarm Package: Img.IK8557582 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-1843 IK8557583

Alarm	Attributes	Applicable major release
Name: IK8557583 (10703) Type: processingErrorAlarm Package: Img.IK8557583 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.		

Table 27-1843 IK8557583 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1844 IK8557584

Alarm	Attributes	Applicable major release
Name: IK8557584 (10704) Type: processingErrorAlarm Package: lmg.IK8557584 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-1845 IK8557585

Alarm	Attributes	Applicable major release
Name: IK8557585 (10705) Type: processingErrorAlarm Package: lmg.IK8557585 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-1846 IK8557586

Alarm	Attributes	Applicable major release
Name: IK8557586 (10706) Type: processingErrorAlarm Package: lmg.IK8557586 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-1847 IK8557587

Alarm	Attributes	Applicable major release
Name: IK8557587 (10707) Type: processingErrorAlarm Package: Img.IK8557587 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-1848 IK8557588

Alarm	Attributes	Applicable major release
Name: IK8557588 (10708) Type: processingErrorAlarm Package: Img.IK8557588 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-1849 IK8557589

Alarm	Attributes	Applicable major release
Name: IK8557589 (10709) Type: processingErrorAlarm Package: Img.IK8557589 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-1850 IK8557590

Alarm	Attributes	Applicable major release
Name: IK8557590 (10710) Type: processingErrorAlarm Package: Img.IK8557590 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-1851 IK8557591

Alarm	Attributes	Applicable major release
Name: IK8557591 (10711) Type: processingErrorAlarm Package: Img.IK8557591 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.		
Remedial action: No action is required.		

Table 27-1852 IK8557592

Alarm	Attributes	Applicable major release
Name: IK8557592 (10712) Type: processingErrorAlarm Package: Img.IK8557592 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-1853 IK8557593

Alarm	Attributes	Applicable major release
Name: IK8557593 (10713) Type: processingErrorAlarm Package: Img.IK8557593 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-1854 IK8557594

Alarm	Attributes	Applicable major release
Name: IK8557594 (10714) Type: processingErrorAlarm Package: Img.IK8557594 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-1854 IK8557594 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-1855 IK8557595

Alarm	Attributes	Applicable major release
Name: IK8557595 (10715) Type: processingErrorAlarm Package: lmg.IK8557595 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.		
Remedial action: No action is required.		

Table 27-1856 IK8557596

Alarm	Attributes	Applicable major release
Name: IK8557596 (10716) Type: processingErrorAlarm Package: lmg.IK8557596 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.		
Remedial action: No action is required.		

Table 27-1857 IK8557597

Alarm	Attributes	Applicable major release
Name: IK8557597 (10717) Type: processingErrorAlarm Package: lmg.IK8557597 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.		
Remedial action: No action is required.		

Table 27-1858 IK8557598

Alarm	Attributes	Applicable major release
Name: IK8557598 (10718) Type: processingErrorAlarm Package: lmg.IK8557598 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.		
Remedial action: No action is required.		

Table 27-1859 IK8557599

Alarm	Attributes	Applicable major release
Name: IK8557599 (10719) Type: processingErrorAlarm Package: lmg.IK8557599 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.		
Remedial action: No action is required.		

Table 27-1860 IK8557600

Alarm	Attributes	Applicable major release
Name: IK8557600 (10720) Type: processingErrorAlarm Package: lmg.IK8557600 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.		
Remedial action: No action is required.		

Table 27-1861 IK8557601

Alarm	Attributes	Applicable major release
Name: IK8557601 (10721) Type: processingErrorAlarm Package: lmg.IK8557601 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.		

Table 27-1861 IK8557601 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-1862 IK8557602

Alarm	Attributes	Applicable major release
Name: IK8557602 (10722) Type: processingErrorAlarm Package: Img.IK8557602 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.		
Remedial action: No action is required.		

Table 27-1863 IK8557603

Alarm	Attributes	Applicable major release
Name: IK8557603 (10723) Type: processingErrorAlarm Package: Img.IK8557603 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.		
Remedial action: No action is required.		

Table 27-1864 IK8557604

Alarm	Attributes	Applicable major release
Name: IK8557604 (10724) Type: processingErrorAlarm Package: Img.IK8557604 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.		
Remedial action: No action is required.		

Table 27-1865 IK8557605

Alarm	Attributes	Applicable major release
Name: IK8557605 (10725) Type: processingErrorAlarm Package: Img.IK8557605 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.		
Remedial action: No action is required.		

Table 27-1866 IK8557606

Alarm	Attributes	Applicable major release
Name: IK8557606 (10726) Type: processingErrorAlarm Package: Img.IK8557606 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.		
Remedial action: No action is required.		

Table 27-1867 IK8557607

Alarm	Attributes	Applicable major release
Name: IK8557607 (10727) Type: processingErrorAlarm Package: Img.IK8557607 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A storage system power supply status has been set to degraded.		
Remedial action: No action is required.		

Table 27-1868 IK8590000

Alarm	Attributes	Applicable major release
Name: IK8590000 (9304) Type: processingErrorAlarm Package: Img.IK8590000 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG

Table 27-1868 IK8590000 (continued)

Alarm	Attributes	Applicable major release
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1869 IK8590001

Alarm	Attributes	Applicable major release
Name: IK8590001 (9305) Type: processingErrorAlarm Package: Img.IK8590001 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1870 IK8590002

Alarm	Attributes	Applicable major release
Name: IK8590002 (9306) Type: processingErrorAlarm Package: Img.IK8590002 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1871 IK8590003

Alarm	Attributes	Applicable major release
Name: IK8590003 (9307) Type: processingErrorAlarm Package: Img.IK8590003 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1872 IK8590004

Alarm	Attributes	Applicable major release
Name: IK8590004 (9308) Type: processingErrorAlarm Package: lmg.IK8590004 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1873 IK8590005

Alarm	Attributes	Applicable major release
Name: IK8590005 (9309) Type: processingErrorAlarm Package: lmg.IK8590005 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1874 IK8590006

Alarm	Attributes	Applicable major release
Name: IK8590006 (9310) Type: processingErrorAlarm Package: lmg.IK8590006 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1875 IK8590007

Alarm	Attributes	Applicable major release
Name: IK8590007 (9311) Type: processingErrorAlarm Package: lmg.IK8590007 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1876 IK8590008

Alarm	Attributes	Applicable major release
Name: IK8590008 (9312) Type: processingErrorAlarm Package: Img.IK8590008 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1877 IK8590009

Alarm	Attributes	Applicable major release
Name: IK8590009 (9313) Type: processingErrorAlarm Package: Img.IK8590009 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1878 IK8590010

Alarm	Attributes	Applicable major release
Name: IK8590010 (9314) Type: processingErrorAlarm Package: Img.IK8590010 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1879 IK8590011

Alarm	Attributes	Applicable major release
Name: IK8590011 (9315) Type: processingErrorAlarm Package: Img.IK8590011 Raised on class: Img.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1880 IK8590012

Alarm	Attributes	Applicable major release
Name: IK8590012 (9316) Type: processingErrorAlarm Package: lmg.IK8590012 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1881 IK8590013

Alarm	Attributes	Applicable major release
Name: IK8590013 (9317) Type: processingErrorAlarm Package: lmg.IK8590013 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1882 IK8590014

Alarm	Attributes	Applicable major release
Name: IK8590014 (9318) Type: processingErrorAlarm Package: lmg.IK8590014 Raised on class: lmg.UPlane	Severity: warning Specific problem: Provision Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-1883 IK8590015

Alarm	Attributes	Applicable major release
Name: IK8590015 (9960) Type: processingErrorAlarm Package: lmg.IK8590015 Raised on class: lmg.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1884 IK8590016

Alarm	Attributes	Applicable major release
Name: IK8590016 (9961) Type: processingErrorAlarm Package: Img.IK8590016 Raised on class: Img.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1885 IK8590017

Alarm	Attributes	Applicable major release
Name: IK8590017 (9962) Type: processingErrorAlarm Package: Img.IK8590017 Raised on class: Img.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1886 IK8590018

Alarm	Attributes	Applicable major release
Name: IK8590018 (9963) Type: processingErrorAlarm Package: Img.IK8590018 Raised on class: Img.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1887 IK8590019

Alarm	Attributes	Applicable major release
Name: IK8590019 (9964) Type: processingErrorAlarm Package: Img.IK8590019 Raised on class: Img.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1888 IK8590020

Alarm	Attributes	Applicable major release
Name: IK8590020 (9965) Type: processingErrorAlarm Package: lmg.IK8590020 Raised on class: lmg.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1889 IK8590021

Alarm	Attributes	Applicable major release
Name: IK8590021 (9966) Type: processingErrorAlarm Package: lmg.IK8590021 Raised on class: lmg.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1890 IK8590022

Alarm	Attributes	Applicable major release
Name: IK8590022 (9967) Type: processingErrorAlarm Package: lmg.IK8590022 Raised on class: lmg.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1891 IK8590023

Alarm	Attributes	Applicable major release
Name: IK8590023 (9968) Type: processingErrorAlarm Package: lmg.IK8590023 Raised on class: lmg.UPlane	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1892 IK8600124

Alarm	Attributes	Applicable major release
Name: IK8600124 (7400) Type: processingErrorAlarm Package: lmg.IK8600124 Raised on class: lmg.Flute	Severity: major Specific problem: Error when trying to add content Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fails to watch the webdav folder for Delivery Instance ID (variable parameters such as webdav folder, DeliveryInstanceId and cause are also indicated)\nReason: Error when trying to add content. Webdav folder deleted by a third party OR delivery instance deleted by a concurrent request		
Remedial action: Check if the delivery instance has been deleted. Check if the instance is still existing on the Broadcast Delivery Server, and that a Delete has not been concurrently performed.		

Table 27-1893 IK8600132

Alarm	Attributes	Applicable major release
Name: IK8600132 (7401) Type: processingErrorAlarm Package: lmg.IK8600132 Raised on class: lmg.Flute	Severity: major Specific problem: Error when trying to delete the directory for a live session - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fails to remove webdav folder for Delivery Instance ID (variable parameters such as webdav folder, DeliveryInstanceId are also indicated)\nReason: Error when trying to delete the directory for a live session - case 1. Webdav folder could not be deleted		
Remedial action: Check that the Broadcast Delivery Server has rights to delete the folder, and that there is no concurrent writing.		

Table 27-1894 IK8600137

Alarm	Attributes	Applicable major release
Name: IK8600137 (7402) Type: processingErrorAlarm Package: lmg.IK8600137 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when trying to create a BmscEvent Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when generating bmsc event string\nReason: Issue occurs when trying to create a BmscEvent. No identified cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1895 IK8600141

Alarm	Attributes	Applicable major release
Name: IK8600141 (7403) Type: processingErrorAlarm Package: lmg.IK8600141 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when trying to get DeliverySession from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery session from database (variable parameters such as deliverySessionId, cause are also indicated)\nReason: Issue occurs when trying to get DeliverySession from database . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1896 IK8600142

Alarm	Attributes	Applicable major release
Name: IK8600142 (7404) Type: processingErrorAlarm Package: lmg.IK8600142 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when trying to get the DeliveryInstance from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery instance from database (variable parameters such as deliveryInstanceId, cause are also indicated)\nReason: Issue occurs when trying to get the DeliveryInstance from database . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1897 IK8600143

Alarm	Attributes	Applicable major release
Name: IK8600143 (7405) Type: processingErrorAlarm Package: lmg.IK8600143 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when trying to get DeliveryInstances from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get Delivery Instances for the Delivery Session (variable parameters such as DeliverySessionId, cause are also indicated)\nReason: Issue occurs when trying to get DeliveryInstances from database. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1898 IK8600146

Alarm	Attributes	Applicable major release
Name: IK8600146 (7406) Type: processingErrorAlarm Package: Img.IK8600146 Raised on class: Img.Flute	Severity: major Specific problem: Issue occurs when trying to get OnDemandContent from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the OnDemand content from database (variable parameters such as ContentId, cause are also indicated)\nReason: Issue occurs when trying to get OnDemandContent from database. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1899 IK8600152

Alarm	Attributes	Applicable major release
Name: IK8600152 (7407) Type: processingErrorAlarm Package: Img.IK8600152 Raised on class: Img.Flute	Severity: critical Specific problem: Problem when initializing the FluteEngine library - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to initialize FluteSender library (variable parameters such as DeliveryInstanceId are also indicated)\nReason: Problem when initializing the FluteEngine library - case 1. Broadcast Delivery Server deployment error or Out of memory, memory leaks on Flute engine		
Remedial action: Stop and reinstall the Broadcast Delivery Server.		

Table 27-1900 IK8600159

Alarm	Attributes	Applicable major release
Name: IK8600159 (7408) Type: processingErrorAlarm Package: Img.IK8600159 Raised on class: Img.Flute	Severity: major Specific problem: Error when trying to create the webdav folder for an instance Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create webdav folder for Delivery Instance ID (variable parameters such as webdavPath, deliveryInstanceId are also indicated)\nReason: Error when trying to create the webdav folder for an instance. Webdav folder could not be created: no rights OR webdav folders path not existing		
Remedial action: Check existence of the base path and that the Broadcast Delivery Server has the creation rights		

Table 27-1901 IK8600163

Alarm	Attributes	Applicable major release
Name: IK8600163 (9319) Type: processingErrorAlarm Package: lmg.IK8600163 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when updating the DeliveryInstance in database. Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Fails to remove content (content variable parameter is also indicated)\nReason: Issue occurs when updating the DeliveryInstance in database. . The database can not be reached or persistence errors - issue occurs when removing content from database		
Remedial action: Check that the mysql database is running.		

Table 27-1902 IK8600164

Alarm	Attributes	Applicable major release
Name: IK8600164 (7409) Type: processingErrorAlarm Package: lmg.IK8600164 Raised on class: lmg.Flute	Severity: major Specific problem: Issue occurs when trying to get DeliverySession with given TSI from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the DeliverySession with tsi (variable parameters such as tsi, cause are also indicated)\nReason: Issue occurs when trying to get DeliverySession with given TSI from database. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1903 IK8600168

Alarm	Attributes	Applicable major release
Name: IK8600168 (7410) Type: processingErrorAlarm Package: lmg.IK8600168 Raised on class: lmg.Flute	Severity: major Specific problem: Database problem - case 1 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery instances - database failure (variable parameters such as cause are also indicated)\nReason: Database problem - case 1. The database can not be reached or persistence errors - issue occurs while reloading Delivery Instances		
Remedial action: Check that the mysql database is running.		

Table 27-1904 IK8600169

Alarm	Attributes	Applicable major release
Name: IK8600169 (7411) Type: processingErrorAlarm Package: Img.IK8600169 Raised on class: Img.Flute	Severity: major Specific problem: The jnotify listener could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to watch webdav folder for Delivery Instance ID (variable parameters such as webdavFolder, DeliveryInstanceId, cause are also indicated)\nReason: The jnotify listener could not be created. No identified cause (issue with Jnotify)		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1905 IK8600170

Alarm	Attributes	Applicable major release
Name: IK8600170 (7412) Type: processingErrorAlarm Package: Img.IK8600170 Raised on class: Img.Flute	Severity: major Specific problem: Database problem - case 2 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to update DeliveryInstance ID (variable parameters such as DeliveryInstanceId, webdavFolder, cause are also indicated)\nReason: Database problem - case 2. The database can not be reached or persistence errors - issue occurs while trying to update Delivery Instance		
Remedial action: Check that the mysql database is running.		

Table 27-1906 IK8600172

Alarm	Attributes	Applicable major release
Name: IK8600172 (7413) Type: processingErrorAlarm Package: Img.IK8600172 Raised on class: Img.Flute	Severity: major Specific problem: Error when trying to delete the directory for a live session - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove webdav folder (variable parameters such as deliveryInstanceId, webdavFolder are also indicated)\ nReason: Error when trying to delete the directory for a live session - case 2 . Webdav folder could not be deleted		
Remedial action: Check that the Broadcast Delivery Server has rights to delete the folder, and that there is no concurrent writing		

Table 27-1907 IK8600174

Alarm	Attributes	Applicable major release
Name: IK8600174 (7414) Type: communicationsAlarm Package: lmg.IK8600174 Raised on class: lmg.Flute	Severity: minor Specific problem: Problem with the url in charge of receiving the events - case 1 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to send event (variable parameters such as event, cause are also indicated)\nReason: Problem with the url in charge of receiving the events - case 1. The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1908 IK8600175

Alarm	Attributes	Applicable major release
Name: IK8600175 (7415) Type: communicationsAlarm Package: lmg.IK8600175 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: case 2 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File_Continous_Failed (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1909 IK8600179

Alarm	Attributes	Applicable major release
Name: IK8600179 (7416) Type: processingErrorAlarm Package: lmg.IK8600179 Raised on class: lmg.Flute	Severity: major Specific problem: Error when trying to delete the directory for a live session Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove webdav folder after delete instance (variable parameters such as deliveryInstanceId, webdavFolder are also indicated)\nReason: Error when trying to delete the directory for a live session. Webdav folder could not be deleted		
Remedial action: Check that the Broadcast Delivery Server has rights to delete the folder, and that there is no concurrent writing		

Table 27-1910 IK8600211

Alarm	Attributes	Applicable major release
Name: IK8600211 (7417) Type: communicationsAlarm Package: Img.IK8600211 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with the url in charge of receiving the events - case 3 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: Fails send event File_Ready_For_Delivery (variable parameters such as cause are also indicated)\nReason: Problem with the url in charge of receiving the events - case 3. The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1911 IK8600214

Alarm	Attributes	Applicable major release
Name: IK8600214 (7418) Type: processingErrorAlarm Package: Img.IK8600214 Raised on class: Img.Flute	Severity: major Specific problem: Problem with database - case 4 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create index (variable parameters such as index, cause are also indicated)\nReason: Problem with database - case 4. The database can not be reached		
Remedial action: Check that the mysql database is running.		

Table 27-1912 IK8600216

Alarm	Attributes	Applicable major release
Name: IK8600216 (7419) Type: processingErrorAlarm Package: Img.IK8600216 Raised on class: Img.Flute	Severity: major Specific problem: Problem with database - case 5 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery sessions from database - database failure (variable parameters such as cause are also indicated)\nReason: Problem with database - case 5. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1913 IK8600217

Alarm	Attributes	Applicable major release
Name: IK8600217 (7420) Type: processingErrorAlarm Package: lmg.IK8600217 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with database - case 6 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the OnDemand files from database (variable parameters such as cause are also indicated)\nReason: Problem with database - case 6. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1914 IK8600234

Alarm	Attributes	Applicable major release
Name: IK8600234 (7421) Type: processingErrorAlarm Package: lmg.IK8600234 Raised on class: lmg.Flute	Severity: minor Specific problem: Problem with server. Properties - case 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of intparameter Use default value instead (variable parameters such as key authorized values, default value are also indicated)\nReason: Problem with server. Properties - case 1. An int parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1915 IK8600236

Alarm	Attributes	Applicable major release
Name: IK8600236 (7422) Type: processingErrorAlarm Package: lmg.IK8600236 Raised on class: lmg.Flute	Severity: minor Specific problem: Problem with server. Properties - case 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of key parameter Use default value instead (variable parameters such as key, authorized values, default value are also indicated)\nReason: Problem with server. Properties - case 2. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1916 IK8600238

Alarm	Attributes	Applicable major release
Name: IK8600238 (7423) Type: processingErrorAlarm Package: Img.IK8600238 Raised on class: Img.Flute	Severity: major Specific problem: Problem with server. Properties. Server. Multicast. Networkinterface is not found Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Missing broadcast IP in server. Properties Use default IP (variable parameters such as ipbroadcast are also indicated)\nReason: Problem with server. Properties. Server. Multicast. Networkinterface is not found . Server. Multicast. Networkinterface is not found in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1917 IK8600239

Alarm	Attributes	Applicable major release
Name: IK8600239 (7424) Type: processingErrorAlarm Package: Img.IK8600239 Raised on class: Img.Flute	Severity: major Specific problem: Problem with server. Properties - case 3 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Network interface not found. Use default loopback interface (variable parameters such as ip, iploopback are also indicated)\nReason: Problem with server. Properties - case 3. Can not occur		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1918 IK8600240

Alarm	Attributes	Applicable major release
Name: IK8600240 (7425) Type: communicationsAlarm Package: Img.IK8600240 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Server. Multicast. Networkinterface does not correspond to an existing network interface Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The given local IPis not one of available server addressIP (variable parameters such as localIP, addressIP are also indicated). Alarm is cleared only after the server restart.\nReason: server.multicast.networkinterface does not correspond to an existing network interface		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1919 IK8600241

Alarm	Attributes	Applicable major release
Name: IK8600241 (7426) Type: communicationsAlarm Package: lmg.IK8600241 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Problem with the server network interfaces Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The given local IP is unknown (variable parameters such as IP are also indicated). Alarm is cleared only after the server restart.\nReason: server.multicast.networkinterface is not a valid IP address		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1920 IK8600242

Alarm	Attributes	Applicable major release
Name: IK8600242 (7427) Type: processingErrorAlarm Package: lmg.IK8600242 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with local IPs Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Cannot get Local IPs\nReason: Problem with local IPs . Unknown cause: the java process can not list of network interfaces. (No identified reasons, never occured. Can be OS, Hardware error)		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1921 IK8600248

Alarm	Attributes	Applicable major release
Name: IK8600248 (7428) Type: processingErrorAlarm Package: lmg.IK8600248 Raised on class: lmg.Flute	Severity: minor Specific problem: Problem with server. Properties - case 4 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter Use default value instead (variable parameters such as key, default value are also indicated)\nReason: Problem with server. Properties - case 4. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1922 IK8600250

Alarm	Attributes	Applicable major release
Name: IK8600250 (7429) Type: processingErrorAlarm Package: Img.IK8600250 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with server. Properties - case 5 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of long parameter inferior to the min authorized value Use default value instead (variable parameters such as key, minimum value, default value are also indicated)\nReason: Problem with server. Properties - case 5. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1923 IK8600251

Alarm	Attributes	Applicable major release
Name: IK8600251 (7430) Type: processingErrorAlarm Package: Img.IK8600251 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with server. Properties - case 6 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter superior to the max authorized value. Use default value instead (variable parameters such as key, maximum value, default value are also indicated)\nReason: Problem with server. Properties - case 6. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1924 IK8600252

Alarm	Attributes	Applicable major release
Name: IK8600252 (7431) Type: processingErrorAlarm Package: Img.IK8600252 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with server. Properties - case 7 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter: not an integer Use default value instead (variable parameters such as key, default value are also indicated)\nReason: Problem with server. Properties - case 7. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1925 IK8600254

Alarm	Attributes	Applicable major release
Name: IK8600254 (7432) Type: processingErrorAlarm Package: Img.IK8600254 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with server. Properties - case 8 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of integer parameter inferior to the min authorized value Use default value instead (variable parameters such as key, minimum value, default value are also indicated)\nReason: Problem with server. Properties - case 8. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1926 IK8600256

Alarm	Attributes	Applicable major release
Name: IK8600256 (9320) Type: processingErrorAlarm Package: Img.IK8600256 Raised on class: Img.Flute	Severity: major Specific problem: Database not available at Broadcast Delivery Server start Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Could not obtain connection to MySQL database (variable parameter such as exception is indicated)\nReason: Database not available at Broadcast Delivery Server start. The database is not available		
Remedial action: Check that the mysql database is running. Check network connection		

Table 27-1927 IK8600258

Alarm	Attributes	Applicable major release
Name: IK8600258 (7433) Type: processingErrorAlarm Package: Img.IK8600258 Raised on class: Img.Flute	Severity: major Specific problem: Input folder for the ondemand instance could not be deleted - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove on-demand folder for DeliveryInstance ID (variable parameters such as instanceFolder, deliveryInstanceId are also indicated)\nReason: Input folder for the ondemand instance could not be deleted - case 1. A third party has deleted manually the folder Or the folder is locked by another process		
Remedial action: Check the folder state.		

Table 27-1928 IK8600259

Alarm	Attributes	Applicable major release
Name: IK8600259 (7434) Type: processingErrorAlarm Package: Img.IK8600259 Raised on class: Img.Flute	Severity: major Specific problem: Cache folder for the ondemand instance could not be deleted - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove on-demand cache folder or DeliveryInstance ID (variable parameters such as instanceFolder, deliveryInstanceId are also indicated)\nReason: Cache folder for the ondemand instance could not be deleted - case 1. A third party has deleted manually the folder Or the folder is locked by another process		
Remedial action: Check the folder state.		

Table 27-1929 IK8600262

Alarm	Attributes	Applicable major release
Name: IK8600262 (7435) Type: processingErrorAlarm Package: Img.IK8600262 Raised on class: Img.Flute	Severity: minor Specific problem: Old flutesession not remove from flutesession list Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Obsolete flute session found Delete flute session (variable parameters such as deliveryInstanceId are also indicated)\nReason: Old flutesession not remove from flutesession list. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1930 IK8600269

Alarm	Attributes	Applicable major release
Name: IK8600269 (7436) Type: processingErrorAlarm Package: Img.IK8600269 Raised on class: Img.Flute	Severity: major Specific problem: Problem with cache folder Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Unable to write FDT file on disk (variable parameters such as xmlFilePath are also indicated)\nReason: Problem with cache folder. The cache folder is unreachable or lock		
Remedial action: Check the folder state.		

Table 27-1931 IK8600271

Alarm	Attributes	Applicable major release
Name: IK8600271 (7437) Type: processingErrorAlarm Package: Img.IK8600271 Raised on class: Img.Flute	Severity: critical Specific problem: Problem when initializing the FluteEngine library - case 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to initialize FluteEngine library (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when initializing the FluteEngine library - case 2. Memory leaks or Flute engine internal error		
Remedial action: Trigger a switchover		

Table 27-1932 IK8600273

Alarm	Attributes	Applicable major release
Name: IK8600273 (7438) Type: communicationsAlarm Package: Img.IK8600273 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: case 5 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File_Delivery_Started (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1933 IK8600274

Alarm	Attributes	Applicable major release
Name: IK8600274 (7439) Type: communicationsAlarm Package: Img.IK8600274 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: case 6 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File_Delivered (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1934 IK8600275

Alarm	Attributes	Applicable major release
Name: IK8600275 (7440) Type: communicationsAlarm Package: lmg.IK8600275 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: case 7 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File_Transmission_stopped (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1935 IK8600276

Alarm	Attributes	Applicable major release
Name: IK8600276 (7441) Type: processingErrorAlarm Package: lmg.IK8600276 Raised on class: lmg.Flute	Severity: major Specific problem: Error when generator the xml in response to the request get Delivery Session Info Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create delivery session info (variable parameters such as cause are also indicated)\nReason: Error when generator the xml in response to the request get Delivery Session Info. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1936 IK8600286

Alarm	Attributes	Applicable major release
Name: IK8600286 (7442) Type: processingErrorAlarm Package: lmg.IK8600286 Raised on class: lmg.Flute	Severity: critical Specific problem: Server. Properties is not found at start-up Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server config file not found in the indicated path\nReason: Server. Properties is not found at start-up. Server. Properties is missing		
Remedial action: Add the server. Properties and restart.		

Table 27-1937 IK8600287

Alarm	Attributes	Applicable major release
Name: IK8600287 (7443) Type: processingErrorAlarm Package: Img.IK8600287 Raised on class: Img.Flute	Severity: critical Specific problem: Server. Properties can not be parsed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server config file invalid\nReason: Server. Properties can not be parsed. Server. Properties format is not valid		
Remedial action: Correction the server. Properties file and restart.		

Table 27-1938 IK8600288

Alarm	Attributes	Applicable major release
Name: IK8600288 (7444) Type: processingErrorAlarm Package: Img.IK8600288 Raised on class: Img.Flute	Severity: critical Specific problem: Server. Properties can not be read Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: exception_msg\nReason: Server. Properties can not be read. Server. Properties is written or deleted while the Broadcast Delivery Server is reading it		
Remedial action: Restart the Broadcast Delivery Server.		

Table 27-1939 IK8600289

Alarm	Attributes	Applicable major release
Name: IK8600289 (7445) Type: communicationsAlarm Package: Img.IK8600289 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: case 8 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File_Transmission_stopped (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-1940 IK8600295

Alarm	Attributes	Applicable major release
Name: IK8600295 (7446) Type: processingErrorAlarm Package: Img.IK8600295 Raised on class: Img.Flute	Severity: major Specific problem: Input folder for the ondemand instance could not be deleted - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove automatically on-demand folder for DeliveryInstance ID (variable parameters such as instanceFolder, deliveryInstanceId are also indicated)\nReason: Input folder for the ondemand instance could not be deleted - case 2. A third party has deleted manually the folder Or the folder is locked by another process		
Remedial action: Check the folder state.		

Table 27-1941 IK8600296

Alarm	Attributes	Applicable major release
Name: IK8600296 (7447) Type: processingErrorAlarm Package: Img.IK8600296 Raised on class: Img.Flute	Severity: major Specific problem: Cache folder for the ondemand instance could not be deleted - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove automatically on-demand cache folder for DeliveryInstance ID (variable parameters such as instanceFolder, deliveryInstanceId are also indicated)\nReason: Cache folder for the ondemand instance could not be deleted - case 2. A third party has deleted manually the folder Or the folder is locked by another process		
Remedial action: Check the folder state.		

Table 27-1942 IK8600297

Alarm	Attributes	Applicable major release
Name: IK8600297 (7448) Type: processingErrorAlarm Package: Img.IK8600297 Raised on class: Img.Flute	Severity: major Specific problem: The jnotify listener could not be created, when reloading all sessions after a restart Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Delivery Instance ID not loaded Could not create webdav listener (variable parameters such as deliveryInstanceId are also indicated)\nReason: The jnotify listener could not be created, when reloading all sessions after a restart. No identified cause (issue with Jnotify)		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1943 IK8600319

Alarm	Attributes	Applicable major release
Name: IK8600319 (7449) Type: processingErrorAlarm Package: lmg.IK8600319 Raised on class: lmg.Flute	Severity: minor Specific problem: File could not be delivered - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to set add file to flute library for Flute session continuous Skip delivering file (variable parameters such as filePath, deliveryInstanceId are also indicated)\nReason: File could not be delivered - case 1. Fec encoding error or Flute engine internal error - Segment can not be added to flute engine		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1944 IK8600320

Alarm	Attributes	Applicable major release
Name: IK8600320 (7450) Type: processingErrorAlarm Package: lmg.IK8600320 Raised on class: lmg.Flute	Severity: minor Specific problem: File could not be delivered - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to set FDT Expire for Flute session continuous (variable parameters such deliveryInstanceId are also indicated)\nReason: File could not be delivered - case 2. Unknown cause - Memory leak or Flute engine internal error		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1945 IK8600323

Alarm	Attributes	Applicable major release
Name: IK8600323 (9321) Type: processingErrorAlarm Package: lmg.IK8600323 Raised on class: lmg.Flute	Severity: critical Specific problem: License file not valid Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: License file cannot be parsed\nReason: License file not valid. License file corrupted		
Remedial action: Check license file checksum		

Table 27-1946 IK8600328

Alarm	Attributes	Applicable major release
Name: IK8600328 (7451) Type: communicationsAlarm Package: Img.IK8600328 Raised on class: Img.Flute	Severity: critical Specific problem: The mulltiFEC library is missing or can be loaded Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Required library not found (variable parameters such as path are also indicated)\nReason: The mulltiFEC library is missing or can be loaded . Missing required libraries		
Remedial action: Check the presence of the *. So libraries		

Table 27-1947 IK8600333

Alarm	Attributes	Applicable major release
Name: IK8600333 (7452) Type: processingErrorAlarm Package: Img.IK8600333 Raised on class: Img.Flute	Severity: minor Specific problem: Problem with existence of the mime. Types file in the /config directory Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when loading MIME_TYPES_FILE Default mime types will be used instead (variable parameters such as Mimetypes file are also indicated)\nReason: Problem with existence of the mime. Types file in the /config directory. The mime. Types is missing.		
Remedial action: Check the format of this file. Add the mime. Types config file and restart the Broadcast Delivery Server.		

Table 27-1948 IK8600334

Alarm	Attributes	Applicable major release
Name: IK8600334 (7453) Type: processingErrorAlarm Package: Img.IK8600334 Raised on class: Img.Flute	Severity: critical Specific problem: License file not found or not valid Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: License file not found or not valid\nReason: License file not found or not valid (cannot be parsed). License file not found		
Remedial action: Check licence file existence.		

Table 27-1949 IK8600335

Alarm	Attributes	Applicable major release
Name: IK8600335 (7454) Type: processingErrorAlarm Package: Img.IK8600335 Raised on class: Img.Flute	Severity: critical Specific problem: Problem with license Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: exception_msg. New License to be ordered\nReason: Problem with license. The license doesn't authorize to run the Broadcast Delivery Server		
Remedial action: Order a new license .		

Table 27-1950 IK8600336

Alarm	Attributes	Applicable major release
Name: IK8600336 (7455) Type: communicationsAlarm Package: Img.IK8600336 Raised on class: Img.Flute	Severity: major Specific problem: Check delivery instance id Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: control fragment session fails to start. Delivery Instance not found (variable parameters such as deliveryInstanceId, cause are also indicated)\nReason: Check delivery instance id. The instance id referenced in the request doesn't exist		
Remedial action: Check the instance Id existence.		

Table 27-1951 IK8600338

Alarm	Attributes	Applicable major release
Name: IK8600338 (7456) Type: processingErrorAlarm Package: Img.IK8600338 Raised on class: Img.Flute	Severity: major Specific problem: Problem when initializing the FluteEngine library - case 3 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to initialize FluteSender library for control fragments (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when initializing the FluteEngine library - case 3. Memory leak or Flute engine internal error		
Remedial action: Stop and reinstall the Broadcast Delivery Server		

Table 27-1952 IK8600339

Alarm	Attributes	Applicable major release
Name: IK8600339 (7457) Type: processingErrorAlarm Package: lmg.IK8600339 Raised on class: lmg.Flute	Severity: major Specific problem: Problem when adding a fragment to the FluteEngine library - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to add fragment to flute library for fragment session. Skip delivering fragment (variable parameters such as file path, delieryInstanceId are also indicated)\nReason: Problem when adding a fragment to the FluteEngine library - case 1. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1953 IK8600340

Alarm	Attributes	Applicable major release
Name: IK8600340 (7458) Type: processingErrorAlarm Package: lmg.IK8600340 Raised on class: lmg.Flute	Severity: major Specific problem: Problem when adding a fragment to the FluteEngine library - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to add fragment to flute library for fragment session. Skip delivering fragment (variable parameters such as file path, delieryInstanceId are also indicated)\nReason: Problem when adding a fragment to the FluteEngine library - case 2. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1954 IK8600341

Alarm	Attributes	Applicable major release
Name: IK8600341 (7459) Type: processingErrorAlarm Package: lmg.IK8600341 Raised on class: lmg.Flute	Severity: major Specific problem: Problem when starting the delivery of the control fragments - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to start transmission cycle for fragment session, Stopping Flute session (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when starting the delivery of the control fragments - case 1. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1955 IK8600343

Alarm	Attributes	Applicable major release
Name: IK8600343 (7460) Type: processingErrorAlarm Package: lmg.IK8600343 Raised on class: lmg.Flute	Severity: major Specific problem: Problem when starting the delivery of the control fragments - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fragments session start failed (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when starting the delivery of the control fragments - case 2. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1956 IK8600346

Alarm	Attributes	Applicable major release
Name: IK8600346 (7461) Type: processingErrorAlarm Package: lmg.IK8600346 Raised on class: lmg.Flute	Severity: major Specific problem: OriginatorUserName can not be blank and can not contains spaces Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of server. Multicast. SDP. Originator parameter (variable parameters such as invalid parameter value, default value are also indicated)\nReason: OriginatorUserName can not be blank and can not contains spaces. Server. Multicast. SDP. Originator is not found or incorrect in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1957 IK8600347

Alarm	Attributes	Applicable major release
Name: IK8600347 (7462) Type: processingErrorAlarm Package: lmg.IK8600347 Raised on class: lmg.Flute	Severity: major Specific problem: No namespace for the control fragments has been configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: No namespace for the control fragments has been configured (variable parameters are also indicated)\nReason: No namespace for the control fragments has been configured. No namespace configured		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-1958 IK8600351

Alarm	Attributes	Applicable major release
Name: IK8600351 (7463) Type: processingErrorAlarm Package: Img.IK8600351 Raised on class: Img.Flute	Severity: major Specific problem: Problem with database - case 8 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Can not queue file for delivery. Cause Fails to get OnDemandFile from database (variable parameters such as file path, cause are also indicated)\nReason: Problem with database - case 8. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1959 IK8600352

Alarm	Attributes	Applicable major release
Name: IK8600352 (7464) Type: processingErrorAlarm Package: Img.IK8600352 Raised on class: Img.Flute	Severity: major Specific problem: A file in delivery queue is no more available in database Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Can not queue file for delivery. Cause OnDemandFile not found in database (variable parameters such as file path are also indicated)\nReason: A file in delivery queue is no more available in database. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1960 IK8600353

Alarm	Attributes	Applicable major release
Name: IK8600353 (7465) Type: processingErrorAlarm Package: Img.IK8600353 Raised on class: Img.Flute	Severity: major Specific problem: Problem with stream file and time offset Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: File not send. Cause FluteEngine fails to read stream (variable parameters such as file path are also indicated). File stream removed from the cache folder, or the delivery of a content, whose delivery should be ended has been restarted\nReason: Problem with stream file and time offset. The computed read offset of the stream is out of stream. Flute engine can not read the stream - Can occur after a BDS restart		
Remedial action: Check the stream file in the cache folder. If the Broadcast Delivery Server has been recently restarted after a long pause, No immediate action is required. If the problem persists, contact NOKIA customer support. to perform.		

Table 27-1961 IK8600354

Alarm	Attributes	Applicable major release
Name: IK8600354 (7466) Type: processingErrorAlarm Package: lmg.IK8600354 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with database - case 9 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: File not updated. Cause Fails to get OnDemandFile from database (variable parameters such as file path are also indicated)\nReason: Problem with database - case 9 . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1962 IK8600355

Alarm	Attributes	Applicable major release
Name: IK8600355 (7467) Type: processingErrorAlarm Package: lmg.IK8600355 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: A file in delivery is no more available in database Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: File not updated. Cause OnDemandFile not found in database (variable parameters such as file path are also indicated). Alarm to be cleared by the operator at the management system.\nReason: Unknown cause		
Remedial action: No action is required.		

Table 27-1963 IK8600356

Alarm	Attributes	Applicable major release
Name: IK8600356 (7468) Type: processingErrorAlarm Package: lmg.IK8600356 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with database - case 10 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to update the OnDemandFile to database (variable parameters such as fileURI, cause are also indicated)\nReason: Problem with database - case 10 . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-1964 IK8600363

Alarm	Attributes	Applicable major release
Name: IK8600363 (7469) Type: processingErrorAlarm Package: Img.IK8600363 Raised on class: Img.Flute	Severity: critical Specific problem: The MIB could not be initialized Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when initializing the MIB (variable parameters such as exception are also indicated)\nReason: The MIB could not be initialized. Various possible causes, to be analyzed according the message		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1965 IK8600369

Alarm	Attributes	Applicable major release
Name: IK8600369 (7470) Type: processingErrorAlarm Package: Img.IK8600369 Raised on class: Img.Flute	Severity: major Specific problem: The on demand session failed to start Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to start transmission cycle for Flute session on-demand. Stopping Flute session (variable parameters such as deliveryInstanceId are also indicated)\nReason: The on demand session failed to start. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1966 IK8600370

Alarm	Attributes	Applicable major release
Name: IK8600370 (7471) Type: processingErrorAlarm Package: Img.IK8600370 Raised on class: Img.Flute	Severity: major Specific problem: The continuous session failed to start Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to start transmission cycle for Flute session continuous . Stopping Flute session (variable parameters such as deliveryInstanceId are also indicated)\nReason: The continuous session failed to start. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1967 IK8600374

Alarm	Attributes	Applicable major release
Name: IK8600374 (9322) Type: processingErrorAlarm Package: Img.IK8600374 Raised on class: Img.Flute	Severity: critical Specific problem: The base ondemand folder could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such OnDemand basepath (variable parameter such as basePathOnDemand is also indicated)\nReason: The base ondemand folder could not be created. The ondemand folder could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-1968 IK8600375

Alarm	Attributes	Applicable major release
Name: IK8600375 (9323) Type: processingErrorAlarm Package: Img.IK8600375 Raised on class: Img.Flute	Severity: critical Specific problem: The base folder for continuous session could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such Continuous basepath (variable parameter such as basePathContinuous is also indicated)\nReason: The base folder for continuous session could not be created. The base folder for continuous session could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-1969 IK8600376

Alarm	Attributes	Applicable major release
Name: IK8600376 (9324) Type: processingErrorAlarm Package: Img.IK8600376 Raised on class: Img.Flute	Severity: critical Specific problem: The base ondemand folder for cache could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such OnDemand cache basepath (variable parameter such as basePathObDemandCache is also indicated)\nReason: The base ondemand folder for cache could not be created. The ondemand folder for cache could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-1970 IK8600377

Alarm	Attributes	Applicable major release
Name: IK8600377 (9325) Type: processingErrorAlarm Package: Img.IK8600377 Raised on class: Img.Flute	Severity: critical Specific problem: The base ondemand folder for file repair could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such FileRepair basepath (variable parameter such as basePathFileRepair is also indicated)\nReason: The base ondemand folder for file repair could not be created. The ondemand folder for file repair could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-1971 IK8600381

Alarm	Attributes	Applicable major release
Name: IK8600381 (9326) Type: processingErrorAlarm Package: Img.IK8600381 Raised on class: Img.Flute	Severity: major Specific problem: Verify database. Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Fails to update the OnDemandFile (variable parameters such as fileURI and cause are also indicated)\nReason: Verify database. . The database can not be reached OR persistence errors		
Remedial action: Check that the mysql database is running		

Table 27-1972 IK8600382

Alarm	Attributes	Applicable major release
Name: IK8600382 (9327) Type: processingErrorAlarm Package: Img.IK8600382 Raised on class: Img.Flute	Severity: major Specific problem: Check server. Properties parameter server. Content. Continuous. Queue. Size Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: File delivery queue for Flute session continuous is full, queue is purged. (variable parameter such as Delivery InstanceId is also indicated)\nReason: Check server. Properties parameter server. Content. Continuous. Queue. Size . The bitrate of the instance is not enough		
Remedial action: Check if files are pushed in the webdav folder too fast comparing to the bitrate, create a instance with a bigger bitrate and delete this one.		

Table 27-1973 IK8600385

Alarm	Attributes	Applicable major release
Name: IK8600385 (10728) Type: processingErrorAlarm Package: lmg.IK8600385 Raised on class: lmg.Flute	Severity: warning Specific problem: File in delivery no more available in database Implicitly cleared: true Default probable cause: corruptData	Release: • LR16.1.MG
Description: File not updated. Cause OnDemandFile not found in database (variable parameters such as file path are also indicated)\nReason: File in delivery no more available in database (already removed). Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-1974 IK8600390

Alarm	Attributes	Applicable major release
Name: IK8600390 (7472) Type: communicationsAlarm Package: lmg.IK8600390 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with FDTRepetitionPeriod and bitrate parameters Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: FDT repetition period shorter than FDT transmission duration (variable parameters such as FDT period, FDT transmission duration, ContentId, . . . Are also indicated)\nReason: Problem with FDTRepetitionPeriod and bitrate parameters. The FDT can not be sent as many times as required with the instance bitrate		
Remedial action: FDTRepetitionPeriod may be too important comparing to the bitrate and FDT size. Check the bitrate of the instance, and the FDT period. Delete the delivery instance. Create another delivery instance with the correct parameters.		

Table 27-1975 IK8600391

Alarm	Attributes	Applicable major release
Name: IK8600391 (7473) Type: processingErrorAlarm Package: lmg.IK8600391 Raised on class: lmg.Flute	Severity: major Specific problem: Problem with server. Properties parameter server. Content. Continuous. Queue. Size Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: File delivery queue for Flute session continuous is full. Files not queued (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem with server. Properties parameter server. Content. Continuous. Queue. Size . The bitrate of the instance is not enough		
Remedial action: Check if files are pushed in the webdav folder too fast comparing to the bitrate, create a instance with a bigger bitrate and delete this one.		

Table 27-1976 IK8600398

Alarm	Attributes	Applicable major release
Name: IK8600398 (7474) Type: communicationsAlarm Package: Img.IK8600398 Raised on class: Img.Flute	Severity: critical Specific problem: Licensing: Authorized maximum bitrate reached - case 1 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Delivery Session reload aborted. Cause Authorized maximum number of sessions reached\nReason: Licensing: Authorized maximum bitrate reached - case 1. The number of sessions in database exceed the authorized number in the licence		
Remedial action: Check the number of registered sessions from database. Use only the right licence.		

Table 27-1977 IK8600399

Alarm	Attributes	Applicable major release
Name: IK8600399 (7475) Type: communicationsAlarm Package: Img.IK8600399 Raised on class: Img.Flute	Severity: critical Specific problem: Licensing: Authorized maximum bitrate reached - case 2 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Delivery Instance reload aborted. Cause Authorized maximum bitrate reached\nReason: Licensing: Authorized maximum bitrate reached - case 2. The total bitrate size for delivery instances exceed the authorized number in the licence		
Remedial action: Check the number of registered instances from database. Use only the right licence.		

Table 27-1978 IK8600407

Alarm	Attributes	Applicable major release
Name: IK8600407 (7476) Type: processingErrorAlarm Package: Img.IK8600407 Raised on class: Img.Flute	Severity: critical Specific problem: An unexpected error occurred during delivery. The delivery is killed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Delivery interrupted for unexpected reason (variable parameters such as delivery instanceId, reason are also indicated)\nReason: An unexpected error occurred during delivery. The delivery is killed. Unknown cause		
Remedial action: Check the message in the error. Perform a deleteContent(abort true) to clean the delivery instance and add again the content to the instance		

Table 27-1979 IK8600408

Alarm	Attributes	Applicable major release
Name: IK8600408 (7477) Type: processingErrorAlarm Package: Img.IK8600408 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The file processing request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: File preparation forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-1980 IK8600409

Alarm	Attributes	Applicable major release
Name: IK8600409 (7478) Type: processingErrorAlarm Package: Img.IK8600409 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The file processing abort request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Abort file preparation forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-1981 IK8600420

Alarm	Attributes	Applicable major release
Name: IK8600420 (9328) Type: processingErrorAlarm Package: Img.IK8600420 Raised on class: Img.Flute	Severity: critical Specific problem: Happen in the DeliveryInstance delete task when database is not reacheable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Unexpected error while getting DeliveryInstance (variable parameters such as delivery instance, cause. . . Are also indicated)\nReason: Happen in the DeliveryInstance delete task when database is not reacheable. The database can not be reached		
Remedial action: Check that the mysql database is running		

Table 27-1982 IK8600440

Alarm	Attributes	Applicable major release
Name: IK8600440 (9329) Type: processingErrorAlarm Package: Img.IK8600440 Raised on class: Img.Flute	Severity: critical Specific problem: Issue occur when trying to add the new event to the events queue Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Event not queued as Events queue full (variable parameter event is also indicated)\nReason: Issue occur when trying to add the new event to the events queue. The events queue is full		
Remedial action: Trigger a swithcover		

Table 27-1983 IK8600443

Alarm	Attributes	Applicable major release
Name: IK8600443 (9330) Type: processingErrorAlarm Package: Img.IK8600443 Raised on class: Img.Flute	Severity: major Specific problem: Occur while reloading delivery instances from db at server restart Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Bitrate taking into account the control fragment bitrate and the synchronisation sequence is too low to transmit at least one packet per SYNC period.\nReason: Occur while reloading delivery instances from db at server restart. The bitrate for Live or Ondemand session is lower than one packet per Minimum Sync Period		
Remedial action: Increase the SYNC sequence then restart the server		

Table 27-1984 IK8600500

Alarm	Attributes	Applicable major release
Name: IK8600500 (9331) Type: processingErrorAlarm Package: Img.IK8600500 Raised on class: Img.Flute	Severity: critical Specific problem: The dongle is not present Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Dongle not found\nReason: The dongle is not present. Dongle removed or not installed		
Remedial action: set up a dongle		

Table 27-1985 IK8600502

Alarm	Attributes	Applicable major release
Name: IK8600502 (9332) Type: processingErrorAlarm Package: Img.IK8600502 Raised on class: Img.Flute	Severity: major Specific problem: Dongle issue Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: USB key protection error\nReason: Dongle issue. Dongle removed or not installed or license limit reached or license expired		
Remedial action: Check the dongle		

Table 27-1986 IK8603228

Alarm	Attributes	Applicable major release
Name: IK8603228 (7479) Type: processingErrorAlarm Package: Img.IK8603228 Raised on class: Img.Flute	Severity: critical Specific problem: License is expired, contact the support to renew the license Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: License is expired.\nReason: License is expired, contact the support to renew the license. License is expired		
Remedial action: Contact NOKIA customer support to renew the license.		

Table 27-1987 IK8603229

Alarm	Attributes	Applicable major release
Name: IK8603229 (7480) Type: processingErrorAlarm Package: Img.IK8603229 Raised on class: Img.Flute	Severity: critical Specific problem: License is invalid. Make sure that all the network interfaces are activated and retry Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Copy protection verification fails.\nReason: License is invalid. Make sure that all the network interfaces are activated and retry. Copy protection verification fails		
Remedial action: Check the server is installed correctly and connected on the network. Contact NOKIA customer support.		

Table 27-1988 IK8603267

Alarm	Attributes	Applicable major release
Name: IK8603267 (7481) Type: processingErrorAlarm Package: Img.IK8603267 Raised on class: Img.Flute	Severity: critical Specific problem: License is invalid, contact the support Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Unknown license for this server\nReason: License is invalid, contact the support. The license doesn't authorize to run the Broadcast Delivery Server		
Remedial action: Order a new license.		

Table 27-1989 IK8609980

Alarm	Attributes	Applicable major release
Name: IK8609980 (10729) Type: processingErrorAlarm Package: Img.IK8609980 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1990 IK8609981

Alarm	Attributes	Applicable major release
Name: IK8609981 (10730) Type: processingErrorAlarm Package: Img.IK8609981 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1991 IK8609982

Alarm	Attributes	Applicable major release
Name: IK8609982 (10731) Type: processingErrorAlarm Package: Img.IK8609982 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-1991 IK8609982 (continued)

Alarm	Attributes	Applicable major release
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1992 IK8609983

Alarm	Attributes	Applicable major release
Name: IK8609983 (10732) Type: processingErrorAlarm Package: lmg.IK8609983 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1993 IK8609984

Alarm	Attributes	Applicable major release
Name: IK8609984 (10733) Type: processingErrorAlarm Package: lmg.IK8609984 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1994 IK8609985

Alarm	Attributes	Applicable major release
Name: IK8609985 (10734) Type: processingErrorAlarm Package: lmg.IK8609985 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1995 IK8609986

Alarm	Attributes	Applicable major release
Name: IK8609986 (10735) Type: processingErrorAlarm Package: Img.IK8609986 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1996 IK8609987

Alarm	Attributes	Applicable major release
Name: IK8609987 (10736) Type: processingErrorAlarm Package: Img.IK8609987 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1997 IK8609988

Alarm	Attributes	Applicable major release
Name: IK8609988 (10737) Type: processingErrorAlarm Package: Img.IK8609988 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1998 IK8609989

Alarm	Attributes	Applicable major release
Name: IK8609989 (10738) Type: processingErrorAlarm Package: Img.IK8609989 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-1999 IK8609990

Alarm	Attributes	Applicable major release
Name: IK8609990 (10739) Type: processingErrorAlarm Package: lmg.IK8609990 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2000 IK8609991

Alarm	Attributes	Applicable major release
Name: IK8609991 (10740) Type: processingErrorAlarm Package: lmg.IK8609991 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2001 IK8609992

Alarm	Attributes	Applicable major release
Name: IK8609992 (10741) Type: processingErrorAlarm Package: lmg.IK8609992 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2002 IK8609993

Alarm	Attributes	Applicable major release
Name: IK8609993 (10742) Type: processingErrorAlarm Package: lmg.IK8609993 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2003 IK8609994

Alarm	Attributes	Applicable major release
Name: IK8609994 (10743) Type: processingErrorAlarm Package: Img.IK8609994 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2004 IK8609995

Alarm	Attributes	Applicable major release
Name: IK8609995 (10744) Type: processingErrorAlarm Package: Img.IK8609995 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2005 IK8609996

Alarm	Attributes	Applicable major release
Name: IK8609996 (10745) Type: processingErrorAlarm Package: Img.IK8609996 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2006 IK8609997

Alarm	Attributes	Applicable major release
Name: IK8609997 (10746) Type: processingErrorAlarm Package: Img.IK8609997 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2007 IK8609998

Alarm	Attributes	Applicable major release
Name: IK8609998 (10747) Type: processingErrorAlarm Package: lmg.IK8609998 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2008 IK8609999

Alarm	Attributes	Applicable major release
Name: IK8609999 (10748) Type: processingErrorAlarm Package: lmg.IK8609999 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2009 IK8610137

Alarm	Attributes	Applicable major release
Name: IK8610137 (7482) Type: processingErrorAlarm Package: lmg.IK8610137 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Issue occurs when trying to create a BmscEvent Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when generating bmsc event string\nReason: Issue occurs when trying to create a BmscEvent. No identified cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2010 IK8610142

Alarm	Attributes	Applicable major release
Name: IK8610142 (7483) Type: processingErrorAlarm Package: lmg.IK8610142 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Issue occurs when trying to get the DeliveryInstance from database Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2010 IK8610142 (continued)

Alarm	Attributes	Applicable major release
Description: Fails to get the delivery instance from database (variable parameters such as deliveryInstanceId, cause are also indicated)\nReason: Issue occurs when trying to get the DeliveryInstance from database . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2011 IK8610168

Alarm	Attributes	Applicable major release
Name: IK8610168 (7484) Type: processingErrorAlarm Package: Img.IK8610168 Raised on class: Img.FilePrepare	Severity: major Specific problem: Database problem - case 1 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery instances - database failure (variable parameters such as cause are also indicated)\nReason: Database problem - case 1. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2012 IK8610174

Alarm	Attributes	Applicable major release
Name: IK8610174 (7485) Type: communicationsAlarm Package: Img.IK8610174 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with the url in charge of receiving the events - case 1 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to send event (variable parameters such as event, cause are also indicated)\nReason: Problem with the url in charge of receiving the events - case 1. The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-2013 IK8610190

Alarm	Attributes	Applicable major release
Name: IK8610190 (7486) Type: processingErrorAlarm Package: Img.IK8610190 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 1 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2013 IK8610190 (continued)

Alarm	Attributes	Applicable major release
Description: Error while saving file to database (variable parameters such as filePath are also indicated)\nReason: Problem with database - case 1. The database can not be reached or persistence errors - issue occurs in ADD CACHE request		
Remedial action: Check that the mysql database is running.		

Table 27-2014 IK8610196

Alarm	Attributes	Applicable major release
Name: IK8610196 (7487) Type: processingErrorAlarm Package: Img.IK8610196 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 2 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get OnDemandFile from database (variable parameters such as URI, fileURI are also indicated)\nReason: Problem with database - case 2. The database can not be reached		
Remedial action: Check that the mysql database is running.		

Table 27-2015 IK8610197

Alarm	Attributes	Applicable major release
Name: IK8610197 (7488) Type: processingErrorAlarm Package: Img.IK8610197 Raised on class: Img.FilePrepare	Severity: major Specific problem: Fails to get the file MD5 from database Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get file uri and MD5 (variable parameters such as URI are also indicated)\nReason: Fails to get the file MD5 from database. Unknown cause		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2016 IK8610200

Alarm	Attributes	Applicable major release
Name: IK8610200 (7489) Type: processingErrorAlarm Package: Img.IK8610200 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 3 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create index. Files not prepared (variable parameters such as index, cause are also indicated)\nReason: Problem with database - case 3. The database can not be reached		

Table 27-2016 IK8610200 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check that the mysql database is running.		

Table 27-2017 IK8610211

Alarm	Attributes	Applicable major release
Name: IK8610211 (7490) Type: communicationsAlarm Package: Img.IK8610211 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with the url in charge of receiving the events - case 3 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to send event (variable parameters such as notification type, cause are also indicated)\nReason: Problem with the url in charge of receiving the events - case 3. The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-2018 IK8610214

Alarm	Attributes	Applicable major release
Name: IK8610214 (7491) Type: processingErrorAlarm Package: Img.IK8610214 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 4 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create index (variable parameters such as index, cause are also indicated)\nReason: Problem with database - case 4. The database can not be reached		
Remedial action: Check that the mysql database is running.		

Table 27-2019 IK8610215

Alarm	Attributes	Applicable major release
Name: IK8610215 (7492) Type: processingErrorAlarm Package: Img.IK8610215 Raised on class: Img.FilePrepare	Severity: major Specific problem: The cache folder is not found, when the Broadcast Delivery Server need to check its free space Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Cache folder is not found or doesn't exists any more\nReason: The cache folder is not found, when the Broadcast Delivery Server need to check its free space. The cache folder is not found or doesn't exists any more		
Remedial action: Check the configuration: server. Content. Ondemand. Cache. Basepath, and the existence of this folder		

Table 27-2020 IK8610216

Alarm	Attributes	Applicable major release
Name: IK8610216 (7493) Type: processingErrorAlarm Package: lmg.IK8610216 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Problem with database - case 5 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the delivery sessions from database - database failure (variable parameters such as cause are also indicated)\nReason: Problem with database - case 5. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2021 IK8610217

Alarm	Attributes	Applicable major release
Name: IK8610217 (7494) Type: processingErrorAlarm Package: lmg.IK8610217 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Problem with database - case 6 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get the OnDemand files from database (variable parameters such as cause are also indicated)\nReason: Problem with database - case 6. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2022 IK8610232

Alarm	Attributes	Applicable major release
Name: IK8610232 (7495) Type: communicationsAlarm Package: lmg.IK8610232 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: case 4 Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Fails to send event File deleted (variable parameters such as cause are also indicated). Alarm is cleared by the system.\nReason: The event could not be sent to the configured URL.		
Remedial action: Check if the URL is correct, and if the orchestrator is correctly started		

Table 27-2023 IK8610234

Alarm	Attributes	Applicable major release
Name: IK8610234 (7496) Type: processingErrorAlarm Package: Img.IK8610234 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of intparameter Use default value instead (variable parameters such as key authorized values, default value are also indicated)\nReason: Problem with server. Properties - case 1. An int parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2024 IK8610236

Alarm	Attributes	Applicable major release
Name: IK8610236 (7497) Type: processingErrorAlarm Package: Img.IK8610236 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of key parameter Use default value instead (variable parameters such as key, authorized values, default value are also indicated)\nReason: Problem with server. Properties - case 2. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2025 IK8610238

Alarm	Attributes	Applicable major release
Name: IK8610238 (7498) Type: communicationsAlarm Package: Img.IK8610238 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with server. Properties. Server. Multicast. Networkinterface is not found Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Missing broadcast IP in server. Properties Use default IP (variable parameters such as ipbroadcast are also indicated)\nReason: Problem with server. Properties. Server. Multicast. Networkinterface is not found . Server. Multicast. Networkinterface is not found in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2026 IK8610239

Alarm	Attributes	Applicable major release
Name: IK8610239 (7499) Type: processingErrorAlarm Package: lmg.IK8610239 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Problem with server. Properties - case 3 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Network interface not found. Use default loopback interface (variable parameters such as ip, iploopback are also indicated)\nReason: Problem with server. Properties - case 3. Can not occur		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2027 IK8610240

Alarm	Attributes	Applicable major release
Name: IK8610240 (7500) Type: communicationsAlarm Package: lmg.IK8610240 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Server. Multicast. Networkinterface does not correspond to an existing network interface Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The given local IPis not one of available server addressIP (variable parameters such as localIP, addressIP are also indicated). Alarm is cleared only after the server restart.\nReason: server.multicast.networkinterface does not correspond to an existing network interface		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2028 IK8610241

Alarm	Attributes	Applicable major release
Name: IK8610241 (7501) Type: communicationsAlarm Package: lmg.IK8610241 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Problem with the server network interfaces Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The given local IP is unknown (variable parameters such as IP are also indicated). Alarm is cleared only after the server restart.\nReason: server.multicast.networkinterface is not a valid IP address		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2029 IK8610242

Alarm	Attributes	Applicable major release
Name: IK8610242 (7502) Type: processingErrorAlarm Package: Img.IK8610242 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with local IPs Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Cannot get Local IPs\nReason: Problem with local IPs . Unknown cause: the java process can not list of network interfaces. (No identified reasons, never occured. Can be OS, Hardware error)		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2030 IK8610248

Alarm	Attributes	Applicable major release
Name: IK8610248 (7503) Type: processingErrorAlarm Package: Img.IK8610248 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 4 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter Use default value instead (variable parameters such as key, default value are also indicated)\nReason: Problem with server. Properties - case 4. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2031 IK8610250

Alarm	Attributes	Applicable major release
Name: IK8610250 (7504) Type: processingErrorAlarm Package: Img.IK8610250 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 5 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of long parameter inferior to the min authorized value Use default value instead (variable parameters such as key, minimum value, default value are also indicated)\nReason: Problem with server. Properties - case 5. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2032 IK8610251

Alarm	Attributes	Applicable major release
Name: IK8610251 (7505) Type: processingErrorAlarm Package: Img.IK8610251 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 6 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter superior to the max authorized value. Use default value instead (variable parameters such as key, maximum value, default value are also indicated)\nReason: Problem with server. Properties - case 6. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2033 IK8610252

Alarm	Attributes	Applicable major release
Name: IK8610252 (7506) Type: processingErrorAlarm Package: Img.IK8610252 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 7 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of parameter: not an integer Use default value instead (variable parameters such as key, default value are also indicated)\nReason: Problem with server. Properties - case 7. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2034 IK8610254

Alarm	Attributes	Applicable major release
Name: IK8610254 (7507) Type: processingErrorAlarm Package: Img.IK8610254 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with server. Properties - case 8 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of integer parameter inferior to the min authorized value Use default value instead (variable parameters such as key, minimum value, default value are also indicated)\nReason: Problem with server. Properties - case 8. An parameter has an invalid value in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2035 IK8610256

Alarm	Attributes	Applicable major release
Name: IK8610256 (9333) Type: processingErrorAlarm Package: Img.IK8610256 Raised on class: Img.FilePrepare	Severity: major Specific problem: Database not available at Broadcast Delivery Server start Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Could not obtain connection to MySQL database (variable parameter such as exception is indicated)\nReason: Database not available at Broadcast Delivery Server start. The database is not available		
Remedial action: Check that the mysql database is running. Check network connection		

Table 27-2036 IK8610271

Alarm	Attributes	Applicable major release
Name: IK8610271 (7508) Type: processingErrorAlarm Package: Img.IK8610271 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Problem when initializing the FluteEngine library - case 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Fails to initialize FluteEngine library (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when initializing the FluteEngine library - case 2. Memory leaks or Flute engine internal error		
Remedial action: Trigger a switchover		

Table 27-2037 IK8610286

Alarm	Attributes	Applicable major release
Name: IK8610286 (7509) Type: processingErrorAlarm Package: Img.IK8610286 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Server. Properties is not found at start-up Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server config file not found in the indicated path\nReason: Server. Properties is not found at start-up. Server. Properties is missing		
Remedial action: Add the server. Properties and restart.		

Table 27-2038 IK8610287

Alarm	Attributes	Applicable major release
Name: IK8610287 (7510) Type: processingErrorAlarm Package: Img.IK8610287 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Server. Properties can not be parsed Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server config file invalid\nReason: Server. Properties can not be parsed. Server. Properties format is not valid		
Remedial action: Correction the server. Properties file and restart.		

Table 27-2039 IK8610288

Alarm	Attributes	Applicable major release
Name: IK8610288 (7511) Type: processingErrorAlarm Package: Img.IK8610288 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Server. Properties can not be read Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: exception_msg\nReason: Server. Properties can not be read. Server. Properties is written or deleted while the Broadcast Delivery Server is reading it		
Remedial action: Restart the Broadcast Delivery Server.		

Table 27-2040 IK8610309

Alarm	Attributes	Applicable major release
Name: IK8610309 (7512) Type: processingErrorAlarm Package: Img.IK8610309 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with database - case 7 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error while removing file from database (variable parameters such as filePath are also indicated)\nReason: Problem with database - case 7. The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2041 IK8610321

Alarm	Attributes	Applicable major release
Name: IK8610321 (7513) Type: processingErrorAlarm Package: Img.IK8610321 Raised on class: Img.FilePrepare	Severity: major Specific problem: File could not be prepared - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to init Flute Stream Generator for OnDemandFile Skip processing file (variable parameters such as filePath, deliveryInstanceId are also indicated)\nReason: File could not be prepared - case 1. Unknown cause - Memory leak or Flute engine internal error		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2042 IK8610322

Alarm	Attributes	Applicable major release
Name: IK8610322 (7514) Type: processingErrorAlarm Package: Img.IK8610322 Raised on class: Img.FilePrepare	Severity: major Specific problem: File could not be prepared - case 2 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to start stream generation process for file (variable parameters such as filePath, deliveryInstanceId are also indicated)\nReason: File could not be prepared - case 2. Unknown cause -Flute engine internal error or disk access problem		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2043 IK8610323

Alarm	Attributes	Applicable major release
Name: IK8610323 (9334) Type: processingErrorAlarm Package: Img.IK8610323 Raised on class: Img.FilePrepare	Severity: critical Specific problem: License file not valid Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: License file cannot be parsed\nReason: License file not valid. License file corrupted		
Remedial action: Check license file checksum		

Table 27-2044 IK8610328

Alarm	Attributes	Applicable major release
Name: IK8610328 (7515) Type: communicationsAlarm Package: Img.IK8610328 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The mulltiFEC library is missing or can be loaded Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Required library not found (variable parameters such as path are also indicated)\nReason: The mulltiFEC library is missing or can be loaded . Missing required libraries		
Remedial action: Check the presence of the *. So libraries		

Table 27-2045 IK8610333

Alarm	Attributes	Applicable major release
Name: IK8610333 (7516) Type: processingErrorAlarm Package: Img.IK8610333 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with existence of the mime. Types file in the /config directory Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when loading MIME_TYPES_FILE Default mime types will be used instead (variable parameters such as Mimetypes file are also indicated)\nReason: Problem with existence of the mime. Types file in the /config directory. The mime. Types is missing.		
Remedial action: Check the format of this file. Add the mime. Types config file and restart the Broadcast Delivery Server.		

Table 27-2046 IK8610334

Alarm	Attributes	Applicable major release
Name: IK8610334 (7517) Type: processingErrorAlarm Package: Img.IK8610334 Raised on class: Img.FilePrepare	Severity: critical Specific problem: License file not found or not valid Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: License file not found or not valid\nReason: License file not found or not valid (cannot be parsed). License file not found		
Remedial action: Check licence file existence.		

Table 27-2047 IK8610335

Alarm	Attributes	Applicable major release
Name: IK8610335 (7518) Type: processingErrorAlarm Package: Img.IK8610335 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Problem with license Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: exception_msg. New License to be ordered\nReason: Problem with license. The license doesn't authorize to run the Broadcast Delivery Server		
Remedial action: Order a new license .		

Table 27-2048 IK8610338

Alarm	Attributes	Applicable major release
Name: IK8610338 (7519) Type: processingErrorAlarm Package: Img.IK8610338 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem when initializing the FluteEngine library - case 3 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fails to initialize FluteSender library for control fragments (variable parameters such as deliveryInstanceId are also indicated)\nReason: Problem when initializing the FluteEngine library - case 3. Memory leak or Flute engine internal error		
Remedial action: Stop and reinstall the Broadcast Delivery Server		

Table 27-2049 IK8610346

Alarm	Attributes	Applicable major release
Name: IK8610346 (7520) Type: processingErrorAlarm Package: Img.IK8610346 Raised on class: Img.FilePrepare	Severity: major Specific problem: OriginatorUserName can not be blank and can not contains spaces Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Invalid value of server. Multicast. SDP. Originator parameter (variable parameters such as invalid parameter value, default value are also indicated)\nReason: OriginatorUserName can not be blank and can not contains spaces. Server. Multicast. SDP. Originator is not found or incorrect in server. Properties		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2050 IK8610347

Alarm	Attributes	Applicable major release
Name: IK8610347 (7521) Type: processingErrorAlarm Package: Img.IK8610347 Raised on class: Img.FilePrepare	Severity: major Specific problem: No namespace for the control fragments has been configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: No namespace for the control fragments has been configured (variable parameters are also indicated)\nReason: No namespace for the control fragments has been configured. No namespace configured		
Remedial action: Correct server. Properties and restart the Broadcast Delivery Server.		

Table 27-2051 IK8610348

Alarm	Attributes	Applicable major release
Name: IK8610348 (7522) Type: processingErrorAlarm Package: Img.IK8610348 Raised on class: Img.FilePrepare	Severity: minor Specific problem: Problem with stop task - case 1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Stop task for flute stream preparation process could not be stopped. Task not registered (variable parameters such as processId are also indicated)\nReason: Problem with stop task - case 1. Internal error		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2052 IK8610350

Alarm	Attributes	Applicable major release
Name: IK8610350 (10749) Type: processingErrorAlarm Package: Img.IK8610350 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 15 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: Delivery Instance ID not found from database. Abort Stop stream preparation task (variable parameter deliveryInstanceId is also indicated)\nReason: Problem with database - case 15 (can happen if instance has been deleted). A delete instance has been done just after a prepare file request on the same instance		
Remedial action: Check that there is no issue in the request callflow performed		

Table 27-2053 IK8610357

Alarm	Attributes	Applicable major release
Name: IK8610357 (7523) Type: processingErrorAlarm Package: Img.IK8610357 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 11 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to create new TOI (Transport Object Identifier) (variable parameters such as cause are also indicated)\nReason: Problem with database - case 11 . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2054 IK8610359

Alarm	Attributes	Applicable major release
Name: IK8610359 (7524) Type: processingErrorAlarm Package: Img.IK8610359 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 12 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to remove TOI (Transport Object Identifier) (variable parameters such as cause are also indicated)\nReason: Problem with database - case 12 . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2055 IK8610360

Alarm	Attributes	Applicable major release
Name: IK8610360 (7525) Type: processingErrorAlarm Package: Img.IK8610360 Raised on class: Img.FilePrepare	Severity: major Specific problem: Problem with database - case 13 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get OnDemanFile count (variable parameters such as cause are also indicated)\nReason: Problem with database - case 13 . The database can not be reached or persistence errors		
Remedial action: Check that the mysql database is running.		

Table 27-2056 IK8610361

Alarm	Attributes	Applicable major release
Name: IK8610361 (7526) Type: processingErrorAlarm Package: lmg.IK8610361 Raised on class: lmg.FilePrepare	Severity: major Specific problem: TOI range [1, 65535] are full Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: TOI (Transport Object Identifier) full\nReason: TOI range [1, 65535] are full. There are near 65535 files in base		
Remedial action: Remove some files before adding new one		

Table 27-2057 IK8610362

Alarm	Attributes	Applicable major release
Name: IK8610362 (7527) Type: processingErrorAlarm Package: lmg.IK8610362 Raised on class: lmg.FilePrepare	Severity: major Specific problem: Problem with database - case 14 Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Fails to get OnDemanFile with TOI (Transport Object Identifier) (variable parameters such as toi, cause are also indicated)\nReason: Problem with database - case 14 . The database can not be reached		
Remedial action: Check that the mysql database is running.		

Table 27-2058 IK8610363

Alarm	Attributes	Applicable major release
Name: IK8610363 (7528) Type: processingErrorAlarm Package: lmg.IK8610363 Raised on class: lmg.FilePrepare	Severity: critical Specific problem: The MIB could not be initialized Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Error when initializing the MIB (variable parameters such as exception are also indicated)\nReason: The MIB could not be initialized. Various possible causes, to be analyzed according the message		
Remedial action: No immediate action is required. If the problem persists, contact NOKIA customer support.		

Table 27-2059 IK8610374

Alarm	Attributes	Applicable major release
Name: IK8610374 (9335) Type: processingErrorAlarm Package: Img.IK8610374 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The base ondemand folder could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such OnDemand basepath (variable parameter such as basePathObDemand is also indicated)\nReason: The base ondemand folder could not be created. The ondemand folder could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-2060 IK8610375

Alarm	Attributes	Applicable major release
Name: IK8610375 (9336) Type: processingErrorAlarm Package: Img.IK8610375 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The base folder for continuous session could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such Continuous basepath (variable parameter such as basePathContinuous is also indicated)\nReason: The base folder for continuous session could not be created. The base folder for continuous session could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-2061 IK8610376

Alarm	Attributes	Applicable major release
Name: IK8610376 (9337) Type: processingErrorAlarm Package: Img.IK8610376 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The base ondemand folder for cache could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such OnDemand cache basepath (variable parameter such as basePathObDemandCache is also indicated)\nReason: The base ondemand folder for cache could not be created. The ondemand folder for cache could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-2062 IK8610377

Alarm	Attributes	Applicable major release
Name: IK8610377 (9338) Type: processingErrorAlarm Package: Img.IK8610377 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The base ondemand folder for file repair could not be created Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: No such FileRepair basepath (variable parameter such as basePathFileRepair is also indicated)\nReason: The base ondemand folder for file repair could not be created. The ondemand folder for file repair could not be created		
Remedial action: Check the folder existence AD/OR the folder creation rights for the BDS on the NAS		

Table 27-2063 IK8610410

Alarm	Attributes	Applicable major release
Name: IK8610410 (7529) Type: processingErrorAlarm Package: Img.IK8610410 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The add content request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Add content forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2064 IK8610411

Alarm	Attributes	Applicable major release
Name: IK8610411 (7530) Type: processingErrorAlarm Package: Img.IK8610411 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The add control fragment request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Add control fragment forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2065 IK8610412

Alarm	Attributes	Applicable major release
Name: IK8610412 (7531) Type: processingErrorAlarm Package: Img.IK8610412 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The remove content request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Remove content forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2066 IK8610413

Alarm	Attributes	Applicable major release
Name: IK8610413 (7532) Type: processingErrorAlarm Package: Img.IK8610413 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The create delivery instance request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Create delivery instance forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2067 IK8610414

Alarm	Attributes	Applicable major release
Name: IK8610414 (7533) Type: processingErrorAlarm Package: Img.IK8610414 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The create delivery session request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Create delivery session forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2068 IK8610415

Alarm	Attributes	Applicable major release
Name: IK8610415 (7534) Type: processingErrorAlarm Package: Img.IK8610415 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The delete delivery instance request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Delete delivery instance forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2069 IK8610416

Alarm	Attributes	Applicable major release
Name: IK8610416 (7535) Type: processingErrorAlarm Package: Img.IK8610416 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The delete delivery session request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Delete delivery session forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2070 IK8610417

Alarm	Attributes	Applicable major release
Name: IK8610417 (7536) Type: processingErrorAlarm Package: Img.IK8610417 Raised on class: Img.LMGMngElement	Severity: major Specific problem: The display delivery session information request returns BAD REQUEST Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Display delivery session information forbidden. Alarm is cleared only after the server restart.\nReason: Misconfiguration		
Remedial action: Check server. Properties server. Flute. Module parameter		

Table 27-2071 IK8610440

Alarm	Attributes	Applicable major release
Name: IK8610440 (9339) Type: processingErrorAlarm Package: Img.IK8610440 Raised on class: Img.FilePrepare	Severity: critical Specific problem: Issue occur when trying to add the new event to the events queue Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Event not queued as Events queue full (variable parameter event is also indicated)\nReason: Issue occur when trying to add the new event to the events queue. The events queue is full		
Remedial action: Trigger a swithcover		

Table 27-2072 IK8610500

Alarm	Attributes	Applicable major release
Name: IK8610500 (9340) Type: processingErrorAlarm Package: Img.IK8610500 Raised on class: Img.FilePrepare	Severity: critical Specific problem: The dongle is not present Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Dongle not found\nReason: The dongle is not present. Dongle removed or not installed		
Remedial action: set up a dongle		

Table 27-2073 IK8610502

Alarm	Attributes	Applicable major release
Name: IK8610502 (9341) Type: processingErrorAlarm Package: Img.IK8610502 Raised on class: Img.FilePrepare	Severity: major Specific problem: Dongle issue Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: USB key protection error\nReason: Dongle issue. Dongle removed or not installed or license limit reached or license expired		
Remedial action: Check the dongle		

Table 27-2074 IK8613228

Alarm	Attributes	Applicable major release
Name: IK8613228 (7537) Type: processingErrorAlarm Package: Img.IK8613228 Raised on class: Img.FilePrepare	Severity: critical Specific problem: License is expired, contact the support to renew the license Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: License is expired.\nReason: License is expired, contact the support to renew the license. License is expired		
Remedial action: Contact NOKIA customer support to renew the license.		

Table 27-2075 IK8613229

Alarm	Attributes	Applicable major release
Name: IK8613229 (7538) Type: processingErrorAlarm Package: Img.IK8613229 Raised on class: Img.FilePrepare	Severity: critical Specific problem: License is invalid. Make sure that all the network interfaces are activated and retry Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Copy protection verification fails.\nReason: License is invalid. Make sure that all the network interfaces are activated and retry. Copy protection verification fails		
Remedial action: Check the server is installed correctly and connected on the network. Contact NOKIA customer support.		

Table 27-2076 IK8613267

Alarm	Attributes	Applicable major release
Name: IK8613267 (7539) Type: processingErrorAlarm Package: Img.IK8613267 Raised on class: Img.FilePrepare	Severity: critical Specific problem: License is invalid, contact the support Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Unknown license for this server\nReason: License is invalid, contact the support. The license doesn't authorize to run the Broadcast Delivery Server		
Remedial action: Order a new license.		

Table 27-2077 IK8619980

Alarm	Attributes	Applicable major release
Name: IK8619980 (10750) Type: processingErrorAlarm Package: Img.IK8619980 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2078 IK8619981

Alarm	Attributes	Applicable major release
Name: IK8619981 (10751) Type: processingErrorAlarm Package: Img.IK8619981 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2079 IK8619982

Alarm	Attributes	Applicable major release
Name: IK8619982 (10752) Type: processingErrorAlarm Package: Img.IK8619982 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2080 IK8619983

Alarm	Attributes	Applicable major release
Name: IK8619983 (10753) Type: processingErrorAlarm Package: Img.IK8619983 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2081 IK8619984

Alarm	Attributes	Applicable major release
Name: IK8619984 (10754) Type: processingErrorAlarm Package: lmg.IK8619984 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2082 IK8619985

Alarm	Attributes	Applicable major release
Name: IK8619985 (10755) Type: processingErrorAlarm Package: lmg.IK8619985 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2083 IK8619986

Alarm	Attributes	Applicable major release
Name: IK8619986 (10756) Type: processingErrorAlarm Package: lmg.IK8619986 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2084 IK8619987

Alarm	Attributes	Applicable major release
Name: IK8619987 (10757) Type: processingErrorAlarm Package: lmg.IK8619987 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2085 IK8619988

Alarm	Attributes	Applicable major release
Name: IK8619988 (10758) Type: processingErrorAlarm Package: lmg.IK8619988 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2086 IK8619989

Alarm	Attributes	Applicable major release
Name: IK8619989 (10759) Type: processingErrorAlarm Package: lmg.IK8619989 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2087 IK8619990

Alarm	Attributes	Applicable major release
Name: IK8619990 (10760) Type: processingErrorAlarm Package: lmg.IK8619990 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2088 IK8619991

Alarm	Attributes	Applicable major release
Name: IK8619991 (10761) Type: processingErrorAlarm Package: lmg.IK8619991 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2089 IK8619992

Alarm	Attributes	Applicable major release
Name: IK8619992 (10762) Type: processingErrorAlarm Package: lmg.IK8619992 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2090 IK8619993

Alarm	Attributes	Applicable major release
Name: IK8619993 (10763) Type: processingErrorAlarm Package: lmg.IK8619993 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2091 IK8619994

Alarm	Attributes	Applicable major release
Name: IK8619994 (10764) Type: processingErrorAlarm Package: lmg.IK8619994 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2092 IK8619995

Alarm	Attributes	Applicable major release
Name: IK8619995 (10765) Type: processingErrorAlarm Package: lmg.IK8619995 Raised on class: lmg.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2093 IK8619996

Alarm	Attributes	Applicable major release
Name: IK8619996 (10766) Type: processingErrorAlarm Package: Img.IK8619996 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2094 IK8619997

Alarm	Attributes	Applicable major release
Name: IK8619997 (10767) Type: processingErrorAlarm Package: Img.IK8619997 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2095 IK8619998

Alarm	Attributes	Applicable major release
Name: IK8619998 (10768) Type: processingErrorAlarm Package: Img.IK8619998 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2096 IK8619999

Alarm	Attributes	Applicable major release
Name: IK8619999 (10769) Type: processingErrorAlarm Package: Img.IK8619999 Raised on class: Img.FilePrepare	Severity: indeterminate Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2097 IK8650005

Alarm	Attributes	Applicable major release
Name: IK8650005 (7540) Type: processingErrorAlarm Package: lmg.IK8650005 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: mcdp alarm trap v1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: mcdp alarm alarm v1.\nAlarm is cleared by the system.\nReason: alarmTrapV1		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2098 IK8650006

Alarm	Attributes	Applicable major release
Name: IK8650006 (7541) Type: processingErrorAlarm Package: lmg.IK8650006 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Trap associated to an alarm of the managed element Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Trap associated to an alarm of the managed element.\nAlarm is cleared by the system when the device is restarted.\nReason: alarmTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2099 IK8650007

Alarm	Attributes	Applicable major release
Name: IK8650007 (7542) Type: processingErrorAlarm Package: lmg.IK8650007 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: softwareFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Trap associated to an alarm while executing software operation (download, activation, validation, reject, backup).\nAlarm is cleared by the system.\nReason: softwareFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2100 IK8650981

Alarm	Attributes	Applicable major release
Name: IK8650981 (7543) Type: equipmentAlarm Package: lmg.IK8650981 Raised on class: lmg.Flute	Severity: minor Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG

Table 27-2100 IK8650981 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm will be sent any time the condition of a node in the cluster becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeDegraded		
Remedial action: Make a note of the cluster node name then check the node for the cause of the degraded condition.		

Table 27-2101 IK8650982

Alarm	Attributes	Applicable major release
Name: IK8650982 (7544) Type: equipmentAlarm Package: lmg.IK8650982 Raised on class: lmg.Flute	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-2102 IK8650983

Alarm	Attributes	Applicable major release
Name: IK8650983 (7545) Type: processingErrorAlarm Package: lmg.IK8650983 Raised on class: lmg.Flute	Severity: minor Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceDegraded		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the degraded condition.		

Table 27-2103 IK8650984

Alarm	Attributes	Applicable major release
Name: IK8650984 (7546) Type: processingErrorAlarm Package: lmg.IK8650984 Raised on class: lmg.Flute	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-2104 IK8650985

Alarm	Attributes	Applicable major release
Name: IK8650985 (7547) Type: equipmentAlarm Package: Img.IK8650985 Raised on class: Img.Flute	Severity: minor Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkDegraded		
Remedial action: Make a note of the cluster network name then check the network for the cause of the degraded condition.		

Table 27-2105 IK8650986

Alarm	Attributes	Applicable major release
Name: IK8650986 (7548) Type: equipmentAlarm Package: Img.IK8650986 Raised on class: Img.Flute	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-2106 IK8650987

Alarm	Attributes	Applicable major release
Name: IK8650987 (7549) Type: environmentalAlarm Package: Img.IK8650987 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The temperature at rack sensor 1 is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmTemp1		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2107 IK8650988

Alarm	Attributes	Applicable major release
Name: IK8650988 (7550) Type: environmentalAlarm Package: Img.IK8650988 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG

Table 27-2107 IK8650988 (continued)

Alarm	Attributes	Applicable major release
Description: The temperature at rack sensor 2 is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmTemp2		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2108 IK8650989

Alarm	Attributes	Applicable major release
Name: IK8650989 (7551) Type: environmentalAlarm Package: lmg.IK8650989 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: The status of Fan 1 has changed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmFan1		
Remedial action: Refer to Trap Details for more information.		

Table 27-2109 IK8650990

Alarm	Attributes	Applicable major release
Name: IK8650990 (7552) Type: environmentalAlarm Package: lmg.IK8650990 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: The status of Fan 2 has changed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmFan2		
Remedial action: Refer to Trap Details for more information.		

Table 27-2110 IK8650991

Alarm	Attributes	Applicable major release
Name: IK8650991 (7553) Type: equipmentAlarm Package: lmg.IK8650991 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The AC voltage of the rack is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmVoltage		
Remedial action: Check the incoming power source and ensure all cables are inserted correctly.		

Table 27-2111 IK8650992

Alarm	Attributes	Applicable major release
Name: IK8650992 (7554) Type: environmentalAlarm Package: Img.IK8650992 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: humidityUnacceptable	Release: • LR14.3.MG
Description: The humidity of the rack is outside the specified threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmHumidity		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2112 IK8650993

Alarm	Attributes	Applicable major release
Name: IK8650993 (7555) Type: environmentalAlarm Package: Img.IK8650993 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #1).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput1		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2113 IK8650994

Alarm	Attributes	Applicable major release
Name: IK8650994 (7556) Type: environmentalAlarm Package: Img.IK8650994 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #2).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput2		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2114 IK8650995

Alarm	Attributes	Applicable major release
Name: IK8650995 (7557) Type: environmentalAlarm Package: Img.IK8650995 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG

Table 27-2114 IK8650995 (continued)

Alarm	Attributes	Applicable major release
Description: The door or sidepanel of the rack has been opened (access point #3).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput3		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2115 IK8650996

Alarm	Attributes	Applicable major release
Name: IK8650996 (7558) Type: environmentalAlarm Package: lmg.IK8650996 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: intrusionDetection	Release: • LR14.3.MG
Description: The door or sidepanel of the rack has been opened (access point #4).\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmInput4		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2116 IK8650997

Alarm	Attributes	Applicable major release
Name: IK8650997 (7559) Type: processingErrorAlarm Package: lmg.IK8650997 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Rack door lock #1 alarm.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock1		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2117 IK8650998

Alarm	Attributes	Applicable major release
Name: IK8650998 (7560) Type: processingErrorAlarm Package: lmg.IK8650998 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: Rack door lock #2 alarm.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock2		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2118 IK8650999

Alarm	Attributes	Applicable major release
Name: IK8650999 (7561) Type: environmentalAlarm Package: lmg.IK8650999 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: smoke	Release: • LR14.3.MG
Description: The rack smoke detector has detected smoke.\nAlarm to be cleared by the operator at the management system.\ nReason: cpqCmcalarmSmoke		
Remedial action: Investigate rack for an over temperature condition and refer to Trap Details for more information.		

Table 27-2119 IK8651000

Alarm	Attributes	Applicable major release
Name: IK8651000 (7562) Type: environmentalAlarm Package: lmg.IK8651000 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: excessiveVibration	Release: • LR14.3.MG
Description: The rack shock detector has detected a vibration to the rack.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmShock		
Remedial action: Investigate rack.		

Table 27-2120 IK8651001

Alarm	Attributes	Applicable major release
Name: IK8651001 (7563) Type: equipmentAlarm Package: lmg.IK8651001 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The rack auxiliary alarm input #1 has been triggered.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmAux1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2121 IK8651002

Alarm	Attributes	Applicable major release
Name: IK8651002 (7564) Type: equipmentAlarm Package: lmg.IK8651002 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2121 IK8651002 (continued)

Alarm	Attributes	Applicable major release
Description: The rack auxiliary alarm input #2 has been triggered.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmAux2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2122 IK8651003

Alarm	Attributes	Applicable major release
Name: IK8651003 (7565) Type: communicationsAlarm Package: lmg.IK8651003 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Alarm 1, set from Network management\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarm1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2123 IK8651004

Alarm	Attributes	Applicable major release
Name: IK8651004 (7566) Type: communicationsAlarm Package: lmg.IK8651004 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: alarm Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Alarm 2, set from Network management\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarm2		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2124 IK8651005

Alarm	Attributes	Applicable major release
Name: IK8651005 (7567) Type: processingErrorAlarm Package: lmg.IK8651005 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm of device Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: The rack door locking device #1 has failed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock1Dev		

Table 27-2124 IK8651005 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-2125 IK8651006

Alarm	Attributes	Applicable major release
Name: IK8651006 (7568) Type: processingErrorAlarm Package: lmg.IK8651006 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: locking-alarm of device Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: The rack door locking device #2 has failed.\nAlarm to be cleared by the operator at the management system.\nReason: cpqCmcalarmLock2Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-2126 IK8651008

Alarm	Attributes	Applicable major release
Name: IK8651008 (7569) Type: equipmentAlarm Package: lmg.IK8651008 Raised on class: lmg.Flute	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2127 IK8651010

Alarm	Attributes	Applicable major release
Name: IK8651010 (7570) Type: equipmentAlarm Package: lmg.IK8651010 Raised on class: lmg.Flute	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2128 IK8651013

Alarm	Attributes	Applicable major release
Name: IK8651013 (7571) Type: equipmentAlarm Package: Img.IK8651013 Raised on class: Img.Flute	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-2129 IK8651015

Alarm	Attributes	Applicable major release
Name: IK8651015 (7572) Type: equipmentAlarm Package: Img.IK8651015 Raised on class: Img.Flute	Severity: minor Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveReducedTrap		
Remedial action: Replace the failed disk device; add a spare to the system to cause a reconstruct.		

Table 27-2130 IK8651018

Alarm	Attributes	Applicable major release
Name: IK8651018 (7573) Type: processingErrorAlarm Package: Img.IK8651018 Raised on class: Img.Flute	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2131 IK8651023

Alarm	Attributes	Applicable major release
Name: IK8651023 (7574) Type: processingErrorAlarm Package: Img.IK8651023 Raised on class: Img.Flute	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-2131 IK8651023 (continued)

Alarm	Attributes	Applicable major release
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2132 IK8651028

Alarm	Attributes	Applicable major release
Name: IK8651028 (7575) Type: environmentalAlarm Package: lmg.IK8651028 Raised on class: lmg.Flute	Severity: minor Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUFanFailureTrap		
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-2133 IK8651030

Alarm	Attributes	Applicable major release
Name: IK8651030 (7576) Type: equipmentAlarm Package: lmg.IK8651030 Raised on class: lmg.Flute	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2134 IK8651032

Alarm	Attributes	Applicable major release
Name: IK8651032 (7577) Type: equipmentAlarm Package: lmg.IK8651032 Raised on class: lmg.Flute	Severity: warning Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUTemperature-WarningTrap		

Table 27-2134 IK8651032 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-2135 IK8651033

Alarm	Attributes	Applicable major release
Name: IK8651033 (7578) Type: equipmentAlarm Package: Img.IK8651033 Raised on class: Img.Flute	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-2136 IK8651035

Alarm	Attributes	Applicable major release
Name: IK8651035 (7579) Type: environmentalAlarm Package: Img.IK8651035 Raised on class: Img.Flute	Severity: minor Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabFanFailureTrap		
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-2137 IK8651037

Alarm	Attributes	Applicable major release
Name: IK8651037 (7580) Type: equipmentAlarm Package: Img.IK8651037 Raised on class: Img.Flute	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2138 IK8651039

Alarm	Attributes	Applicable major release
Name: IK8651039 (7581) Type: environmentalAlarm Package: lmg.IK8651039 Raised on class: lmg.Flute	Severity: warning Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabTemperatureWarningTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-2139 IK8651040

Alarm	Attributes	Applicable major release
Name: IK8651040 (7582) Type: environmentalAlarm Package: lmg.IK8651040 Raised on class: lmg.Flute	Severity: critical Specific problem: cpqCrExpCabTemperatureCriticalTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-2140 IK8651059

Alarm	Attributes	Applicable major release
Name: IK8651059 (7583) Type: equipmentAlarm Package: lmg.IK8651059 Raised on class: lmg.Flute	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2141 IK8651060

Alarm	Attributes	Applicable major release
Name: IK8651060 (7584) Type: environmentalAlarm Package: Img.IK8651060 Raised on class: Img.Flute	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2142 IK8651067

Alarm	Attributes	Applicable major release
Name: IK8651067 (7585) Type: equipmentAlarm Package: Img.IK8651067 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Fibre Channel Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Fibre Channel Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqFcTapeDriveCleanTapeReplace		
Remedial action: Replace the failing fibre channel drive cleaning tape		

Table 27-2143 IK8651068

Alarm	Attributes	Applicable major release
Name: IK8651068 (7586) Type: processingErrorAlarm Package: Img.IK8651068 Raised on class: Img.Flute	Severity: warning Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Redundant Controller Active. This alarm signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-2144 IK8651072

Alarm	Attributes	Applicable major release
Name: IK8651072 (7587) Type: equipmentAlarm Package: Img.IK8651072 Raised on class: Img.Flute	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2145 IK8651073

Alarm	Attributes	Applicable major release
Name: IK8651073 (7588) Type: environmentalAlarm Package: Img.IK8651073 Raised on class: Img.Flute	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2146 IK8651078

Alarm	Attributes	Applicable major release
Name: IK8651078 (7589) Type: processingErrorAlarm Package: Img.IK8651078 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: External Tape Drive Cleaning Required Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG
Description: External Tape Drive Cleaning Required. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm to be cleared by the operator at the management system.\nReason: cpqExtTapeDriveCleaningRequired		
Remedial action: a External Tape Drive Cleaning should be installed		

Table 27-2147 IK8651079

Alarm	Attributes	Applicable major release
Name: IK8651079 (7590) Type: equipmentAlarm Package: Img.IK8651079 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: External Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: External Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqExtTapeDriveCleanTapeReplace		
Remedial action: Replace the External Tape Drive Cleaning Tape		

Table 27-2148 IK8651088

Alarm	Attributes	Applicable major release
Name: IK8651088 (9342) Type: environmentalAlarm Package: Img.IK8651088 Raised on class: Img.Flute	Severity: minor Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHeThermalTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2149 IK8651089

Alarm	Attributes	Applicable major release
Name: IK8651089 (7591) Type: environmentalAlarm Package: Img.IK8651089 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Thermal Status Degraded Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: The temperature status has been set to degraded. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeThermalTempDegraded		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2150 IK8651091

Alarm	Attributes	Applicable major release
Name: IK8651091 (9343) Type: environmentalAlarm Package: lmg.IK8651091 Raised on class: lmg.Flute	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2151 IK8651092

Alarm	Attributes	Applicable major release
Name: IK8651092 (7592) Type: environmentalAlarm Package: lmg.IK8651092 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: System Fan Degraded Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: The system fan status has been set to degraded. An optional system fan is not operating normally.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeThermalSystemFanDegraded		
Remedial action: check the system fans		

Table 27-2152 IK8651094

Alarm	Attributes	Applicable major release
Name: IK8651094 (7593) Type: environmentalAlarm Package: lmg.IK8651094 Raised on class: lmg.Flute	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHeThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2153 IK8651098

Alarm	Attributes	Applicable major release
Name: IK8651098 (7594) Type: equipmentAlarm Package: Img.IK8651098 Raised on class: Img.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2154 IK8651099

Alarm	Attributes	Applicable major release
Name: IK8651099 (7595) Type: equipmentAlarm Package: Img.IK8651099 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Server Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHeFltTolPwrSupplyDegraded		
Remedial action: check the fault tolerant power supply		

Table 27-2155 IK8651102

Alarm	Attributes	Applicable major release
Name: IK8651102 (7596) Type: environmentalAlarm Package: Img.IK8651102 Raised on class: Img.Flute	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2156 IK8651103

Alarm	Attributes	Applicable major release
Name: IK8651103 (7597) Type: environmentalAlarm Package: Img.IK8651103 Raised on class: Img.Flute	Severity: minor Specific problem: Temperature Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2156 IK8651103 (continued)

Alarm	Attributes	Applicable major release
Description: The temperature status has been set to degraded. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2157 IK8651105

Alarm	Attributes	Applicable major release
Name: IK8651105 (7598) Type: environmentalAlarm Package: Img.IK8651105 Raised on class: Img.Flute	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2158 IK8651106

Alarm	Attributes	Applicable major release
Name: IK8651106 (7599) Type: environmentalAlarm Package: Img.IK8651106 Raised on class: Img.Flute	Severity: minor Specific problem: System Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to degraded. An optional system fan is not operating normally.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2159 IK8651108

Alarm	Attributes	Applicable major release
Name: IK8651108 (7600) Type: environmentalAlarm Package: Img.IK8651108 Raised on class: Img.Flute	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2159 IK8651108 (continued)

Alarm	Attributes	Applicable major release
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2160 IK8651112

Alarm	Attributes	Applicable major release
Name: IK8651112 (7601) Type: equipmentAlarm Package: Img.IK8651112 Raised on class: Img.Flute	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2161 IK8651113

Alarm	Attributes	Applicable major release
Name: IK8651113 (7602) Type: equipmentAlarm Package: Img.IK8651113 Raised on class: Img.Flute	Severity: minor Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolPwrSupplyDegraded		
Remedial action: Check the system for a power supply failure. Replace the power supply.		

Table 27-2162 IK8651114

Alarm	Attributes	Applicable major release
Name: IK8651114 (7603) Type: processingErrorAlarm Package: Img.IK8651114 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Corr Mem Errors Require a Replacement Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: A correctable memory log entry indicates a memory module needs to be replaced. The errors have been corrected, but the memory module should be replaced. The error information is reported in the variable cpqHeCorrMemErrDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe3CorrMemReplaceMemModule		

Table 27-2162 IK8651114 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the failing memory module		

Table 27-2163 IK8651116

Alarm	Attributes	Applicable major release
Name: IK8651116 (7604) Type: equipmentAlarm Package: lmg.IK8651116 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2164 IK8651117

Alarm	Attributes	Applicable major release
Name: IK8651117 (7605) Type: equipmentAlarm Package: lmg.IK8651117 Raised on class: lmg.Flute	Severity: minor Specific problem: Power Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The Fault Tolerant Power Supplies have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerRedundancyLost		
Remedial action: Check the system power supplies for a failure.		

Table 27-2165 IK8651120

Alarm	Attributes	Applicable major release
Name: IK8651120 (7606) Type: environmentalAlarm Package: lmg.IK8651120 Raised on class: lmg.Flute	Severity: minor Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2166 IK8651121

Alarm	Attributes	Applicable major release
Name: IK8651121 (7607) Type: environmentalAlarm Package: Img.IK8651121 Raised on class: Img.Flute	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2167 IK8651122

Alarm	Attributes	Applicable major release
Name: IK8651122 (7608) Type: environmentalAlarm Package: Img.IK8651122 Raised on class: Img.Flute	Severity: minor Specific problem: Fan Redundancy Lost Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The Fault Tolerant Fans have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolFanRedundancyLost		
Remedial action: Check the system fans for a failure.		

Table 27-2168 IK8651125

Alarm	Attributes	Applicable major release
Name: IK8651125 (7609) Type: environmentalAlarm Package: Img.IK8651125 Raised on class: Img.Flute	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2169 IK8651126

Alarm	Attributes	Applicable major release
Name: IK8651126 (7610) Type: environmentalAlarm Package: Img.IK8651126 Raised on class: Img.Flute	Severity: minor Specific problem: Thermal Status Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to degraded in the specified chassis and location. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2170 IK8651128

Alarm	Attributes	Applicable major release
Name: IK8651128 (7611) Type: equipmentAlarm Package: Img.IK8651128 Raised on class: Img.Flute	Severity: minor Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterDegraded		
Remedial action: Check for a failing power converter or for a failed power converter in a redundant pair. Replace the power converter.		

Table 27-2171 IK8651129

Alarm	Attributes	Applicable major release
Name: IK8651129 (7612) Type: equipmentAlarm Package: Img.IK8651129 Raised on class: Img.Flute	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-2172 IK8651130

Alarm	Attributes	Applicable major release
Name: IK8651130 (7613) Type: equipmentAlarm Package: Img.IK8651130 Raised on class: Img.Flute	Severity: warning Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterRedundancyLost		
Remedial action: Check the power converters in the system for a failure in a redundant pair. Replace the power converter.		

Table 27-2173 IK8651131

Alarm	Attributes	Applicable major release
Name: IK8651131 (7614) Type: communicationsAlarm Package: Img.IK8651131 Raised on class: Img.Flute	Severity: minor Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR14.3.MG • LR15.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3CacheAccelParityError		
Remedial action: Refer to the Integrated Management Log for details on the error. Replace the cache module.		

Table 27-2174 IK8651132

Alarm	Attributes	Applicable major release
Name: IK8651132 (7615) Type: processingErrorAlarm Package: Img.IK8651132 Raised on class: Img.Flute	Severity: warning Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemOnlineSpareEngaged		
Remedial action: Schedule server down-time to replace the faulty memory.		

Table 27-2175 IK8651134

Alarm	Attributes	Applicable major release
Name: IK8651134 (7616) Type: equipmentAlarm Package: Img.IK8651134 Raised on class: Img.Flute	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to degraded for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2176 IK8651135

Alarm	Attributes	Applicable major release
Name: IK8651135 (7617) Type: equipmentAlarm Package: Img.IK8651135 Raised on class: Img.Flute	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2177 IK8651136

Alarm	Attributes	Applicable major release
Name: IK8651136 (7618) Type: processingErrorAlarm Package: Img.IK8651136 Raised on class: Img.Flute	Severity: warning Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemMirroredMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2178 IK8651137

Alarm	Attributes	Applicable major release
Name: IK8651137 (7619) Type: processingErrorAlarm Package: Img.IK8651137 Raised on class: Img.Flute	Severity: warning Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientAdvancedECCMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2179 IK8651138

Alarm	Attributes	Applicable major release
Name: IK8651138 (7620) Type: processingErrorAlarm Package: Img.IK8651138 Raised on class: Img.Flute	Severity: warning Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemXorMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2180 IK8651141

Alarm	Attributes	Applicable major release
Name: IK8651141 (7621) Type: processingErrorAlarm Package: Img.IK8651141 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Replace Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: Corrected Memory Errors Detected. The errors have been corrected, but the memory module should be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe4CorrMemReplaceMemModule		
Remedial action: Replace the memory module.		

Table 27-2181 IK8651142

Alarm	Attributes	Applicable major release
Name: IK8651142 (7622) Type: equipmentAlarm Package: Img.IK8651142 Raised on class: Img.Flute	Severity: warning Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardRemoved		
Remedial action: Insure the board or cartridge has memory correctly installed and re-insert the memory board or cartridge back into the system.		

Table 27-2182 IK8651144

Alarm	Attributes	Applicable major release
Name: IK8651144 (7623) Type: processingErrorAlarm Package: Img.IK8651144 Raised on class: Img.Flute	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-2183 IK8651148

Alarm	Attributes	Applicable major release
Name: IK8651148 (7624) Type: equipmentAlarm Package: Img.IK8651148 Raised on class: Img.Flute	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-2184 IK8651149

Alarm	Attributes	Applicable major release
Name: IK8651149 (7625) Type: processingErrorAlarm Package: lmg.IK8651149 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Replace Memory Module Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: Corrected \ uncorrected Memory Errors Detected. The errors have been corrected, but the memory module should be replaced. Value 0 for CPU means memory is not Processor based\nAlarm to be cleared by the operator at the management system.\nReason: cpqHe5CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module.		

Table 27-2185 IK8651150

Alarm	Attributes	Applicable major release
Name: IK8651150 (7626) Type: equipmentAlarm Package: lmg.IK8651150 Raised on class: lmg.Flute	Severity: warning Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardRemoved		
Remedial action: Insure the board or cartridge or riser has memory correctly installed and re-insert the memory board or cartridge or CPU back into the system.		

Table 27-2186 IK8651152

Alarm	Attributes	Applicable major release
Name: IK8651152 (7627) Type: processingErrorAlarm Package: lmg.IK8651152 Raised on class: lmg.Flute	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-2187 IK8651153

Alarm	Attributes	Applicable major release
Name: IK8651153 (7628) Type: processingErrorAlarm Package: Img.IK8651153 Raised on class: Img.Flute	Severity: warning Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemLockStepMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2188 IK8651154

Alarm	Attributes	Applicable major release
Name: IK8651154 (7629) Type: equipmentAlarm Package: Img.IK8651154 Raised on class: Img.Flute	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-2189 IK8651156

Alarm	Attributes	Applicable major release
Name: IK8651156 (7630) Type: processingErrorAlarm Package: Img.IK8651156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2190 IK8651158

Alarm	Attributes	Applicable major release
Name: IK8651158 (7631) Type: processingErrorAlarm Package: lmg.IK8651158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2191 IK8651160

Alarm	Attributes	Applicable major release
Name: IK8651160 (9344) Type: communicationsAlarm Package: lmg.IK8651160 Raised on class: lmg.Flute	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2192 IK8651163

Alarm	Attributes	Applicable major release
Name: IK8651163 (7632) Type: communicationsAlarm Package: lmg.IK8651163 Raised on class: lmg.Flute	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2193 IK8651164

Alarm	Attributes	Applicable major release
Name: IK8651164 (7633) Type: communicationsAlarm Package: lmg.IK8651164 Raised on class: lmg.Flute	Severity: warning Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the configured redundant NIC becomes the active NIC.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHo2NicSwitchoverOccurred2		
Remedial action: Examine the network connections and check for a NIC failure.		

Table 27-2194 IK8651168

Alarm	Attributes	Applicable major release
Name: IK8651168 (7634) Type: processingErrorAlarm Package: lmg.IK8651168 Raised on class: lmg.Flute	Severity: warning Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is a send to the user to notify him of a Critical Software Update.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHoCriticalSoftwareUpdateTrap		
Remedial action: Install the required software updates.		

Table 27-2195 IK8651172

Alarm	Attributes	Applicable major release
Name: IK8651172 (7635) Type: qualityOfServiceAlarm Package: lmg.IK8651172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2196 IK8652265

Alarm	Attributes	Applicable major release
Name: IK8652265 (7636) Type: environmentalAlarm Package: lmg.IK8652265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2197 IK8652272

Alarm	Attributes	Applicable major release
Name: IK8652272 (7637) Type: environmentalAlarm Package: lmg.IK8652272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2198 IK8652279

Alarm	Attributes	Applicable major release
Name: IK8652279 (7638) Type: environmentalAlarm Package: lmg.IK8652279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2199 IK8652281

Alarm	Attributes	Applicable major release
Name: IK8652281 (7639) Type: processingErrorAlarm Package: Img.IK8652281 Raised on class: Img.Flute	Severity: warning Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Controller Active. This alarm signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-2200 IK8652284

Alarm	Attributes	Applicable major release
Name: IK8652284 (7640) Type: equipmentAlarm Package: Img.IK8652284 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa4PhyDrvThreshPassedTrap		
Remedial action: If the physical drive is predicting failure, replace the drive.		

Table 27-2201 IK8652289

Alarm	Attributes	Applicable major release
Name: IK8652289 (7641) Type: equipmentAlarm Package: Img.IK8652289 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaTapeDriveCleanTapeReplace		
Remedial action: Replace the Tape Drive Cleaning Tape.		

Table 27-2202 IK8652291

Alarm	Attributes	Applicable major release
Name: IK8652291 (7642) Type: equipmentAlarm Package: Img.IK8652291 Raised on class: Img.Flute	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2203 IK8652292

Alarm	Attributes	Applicable major release
Name: IK8652292 (7643) Type: environmentalAlarm Package: Img.IK8652292 Raised on class: Img.Flute	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2204 IK8652295

Alarm	Attributes	Applicable major release
Name: IK8652295 (7644) Type: equipmentAlarm Package: Img.IK8652295 Raised on class: Img.Flute	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2205 IK8652302

Alarm	Attributes	Applicable major release
Name: IK8652302 (7645) Type: equipmentAlarm Package: Img.IK8652302 Raised on class: Img.Flute	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2206 IK8652304

Alarm	Attributes	Applicable major release
Name: IK8652304 (7646) Type: equipmentAlarm Package: Img.IK8652304 Raised on class: Img.Flute	Severity: minor Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Cache Module Board Bad Data. This alarm signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2207 IK8652305

Alarm	Attributes	Applicable major release
Name: IK8652305 (7647) Type: environmentalAlarm Package: Img.IK8652305 Raised on class: Img.Flute	Severity: minor Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Cache Module Board Backup Power Source Failed. This alarm signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBatteryFailed		
Remedial action: Replace the Backup Power Source.		

Table 27-2208 IK8652309

Alarm	Attributes	Applicable major release
Name: IK8652309 (7648) Type: processingErrorAlarm Package: Img.IK8652309 Raised on class: Img.Flute	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-2209 IK8652310

Alarm	Attributes	Applicable major release
Name: IK8652310 (7649) Type: equipmentAlarm Package: Img.IK8652310 Raised on class: Img.Flute	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-2210 IK8652315

Alarm	Attributes	Applicable major release
Name: IK8652315 (7650) Type: equipmentAlarm Package: Img.IK8652315 Raised on class: Img.Flute	Severity: minor Specific problem: IDE Drive Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: An IDE drive status has been set to degraded.\nAlarm is cleared by the system.\nReason: cpqIdeDriveDegraded		
Remedial action: The drive should be scheduled for replacement. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2211 IK8652317

Alarm	Attributes	Applicable major release
Name: IK8652317 (7651) Type: equipmentAlarm Package: lmg.IK8652317 Raised on class: lmg.Flute	Severity: minor Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqIdeDriveUltraAtaDegraded		
Remedial action: For best performance move Ultra ATA devices to the primary controller and non Ultra ATA devices to the secondary controller. If errors still persist, consider replacing the standard 40-conductor IDE cable with an 80-conductor Ultra ATA cable.		

Table 27-2212 IK8652337

Alarm	Attributes	Applicable major release
Name: IK8652337 (7652) Type: communicationsAlarm Package: lmg.IK8652337 Raised on class: lmg.Flute	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2213 IK8652339

Alarm	Attributes	Applicable major release
Name: IK8652339 (7653) Type: communicationsAlarm Package: lmg.IK8652339 Raised on class: lmg.Flute	Severity: minor Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicRedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2214 IK8652341

Alarm	Attributes	Applicable major release
Name: IK8652341 (7654) Type: communicationsAlarm Package: Img.IK8652341 Raised on class: Img.Flute	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2215 IK8652343

Alarm	Attributes	Applicable major release
Name: IK8652343 (7655) Type: communicationsAlarm Package: Img.IK8652343 Raised on class: Img.Flute	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2216 IK8652344

Alarm	Attributes	Applicable major release
Name: IK8652344 (7656) Type: communicationsAlarm Package: Img.IK8652344 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: like Activity Detected Trap Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: This alarm will be sent when the Virus Throttle Filter Driver detects virus like activity.\nAlarm to be cleared by the operator at the management system.\nReason: cpqNicVirusLikeActivityDetected		
Remedial action: The system reporting this trap requires immediate attention.		

Table 27-2217 IK8652347

Alarm	Attributes	Applicable major release
Name: IK8652347 (7657) Type: communicationsAlarm Package: lmg.IK8652347 Raised on class: lmg.Flute	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2218 IK8652349

Alarm	Attributes	Applicable major release
Name: IK8652349 (7658) Type: communicationsAlarm Package: lmg.IK8652349 Raised on class: lmg.Flute	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2219 IK8652360

Alarm	Attributes	Applicable major release
Name: IK8652360 (7659) Type: equipmentAlarm Package: lmg.IK8652360 Raised on class: lmg.Flute	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-2220 IK8652361

Alarm	Attributes	Applicable major release
Name: IK8652361 (7660) Type: equipmentAlarm Package: Img.IK8652361 Raised on class: Img.Flute	Severity: minor Specific problem: Enclosure temperature degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to degraded. This alarm signifies that an enclosure temperature sensor has been tripped indicating a possible overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempDegraded		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-2221 IK8652363

Alarm	Attributes	Applicable major release
Name: IK8652363 (7661) Type: environmentalAlarm Package: Img.IK8652363 Raised on class: Img.Flute	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2222 IK8652364

Alarm	Attributes	Applicable major release
Name: IK8652364 (7662) Type: environmentalAlarm Package: Img.IK8652364 Raised on class: Img.Flute	Severity: minor Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to degraded. This alarm signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2223 IK8652368

Alarm	Attributes	Applicable major release
Name: IK8652368 (7663) Type: equipmentAlarm Package: Img.IK8652368 Raised on class: Img.Flute	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2224 IK8652369

Alarm	Attributes	Applicable major release
Name: IK8652369 (7664) Type: equipmentAlarm Package: Img.IK8652369 Raised on class: Img.Flute	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2225 IK8652373

Alarm	Attributes	Applicable major release
Name: IK8652373 (7665) Type: equipmentAlarm Package: Img.IK8652373 Raised on class: Img.Flute	Severity: minor Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem is no longer in a redundant state.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemNotRedundant		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-2226 IK8652374

Alarm	Attributes	Applicable major release
Name: IK8652374 (7666) Type: equipmentAlarm Package: Img.IK8652374 Raised on class: Img.Flute	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-2227 IK8652375

Alarm	Attributes	Applicable major release
Name: IK8652375 (7667) Type: equipmentAlarm Package: Img.IK8652375 Raised on class: Img.Flute	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-2228 IK8652376

Alarm	Attributes	Applicable major release
Name: IK8652376 (7668) Type: equipmentAlarm Package: Img.IK8652376 Raised on class: Img.Flute	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-2229 IK8652377

Alarm	Attributes	Applicable major release
Name: IK8652377 (7669) Type: equipmentAlarm Package: lmg.IK8652377 Raised on class: lmg.Flute	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-2230 IK8652378

Alarm	Attributes	Applicable major release
Name: IK8652378 (7670) Type: equipmentAlarm Package: lmg.IK8652378 Raised on class: lmg.Flute	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-2231 IK8652379

Alarm	Attributes	Applicable major release
Name: IK8652379 (7671) Type: equipmentAlarm Package: lmg.IK8652379 Raised on class: lmg.Flute	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-2232 IK8652380

Alarm	Attributes	Applicable major release
Name: IK8652380 (7672) Type: equipmentAlarm Package: Img.IK8652380 Raised on class: Img.Flute	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-2233 IK8652382

Alarm	Attributes	Applicable major release
Name: IK8652382 (7673) Type: environmentalAlarm Package: Img.IK8652382 Raised on class: Img.Flute	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-2234 IK8652385

Alarm	Attributes	Applicable major release
Name: IK8652385 (7674) Type: equipmentAlarm Package: Img.IK8652385 Raised on class: Img.Flute	Severity: minor Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisNotLoadBalanced		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies. Add additional power supplies if needed.		

Table 27-2235 IK8652386

Alarm	Attributes	Applicable major release
Name: IK8652386 (7675) Type: equipmentAlarm Package: Img.IK8652386 Raised on class: Img.Flute	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2236 IK8652387

Alarm	Attributes	Applicable major release
Name: IK8652387 (7676) Type: equipmentAlarm Package: Img.IK8652387 Raised on class: Img.Flute	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2237 IK8652388

Alarm	Attributes	Applicable major release
Name: IK8652388 (7677) Type: equipmentAlarm Package: Img.IK8652388 Raised on class: Img.Flute	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2238 IK8652389

Alarm	Attributes	Applicable major release
Name: IK8652389 (7678) Type: equipmentAlarm Package: Img.IK8652389 Raised on class: Img.Flute	Severity: minor Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisLoadBalancingWireMissing		
Remedial action: Connect the load balancing wire.		

Table 27-2239 IK8652390

Alarm	Attributes	Applicable major release
Name: IK8652390 (7679) Type: equipmentAlarm Package: Img.IK8652390 Raised on class: Img.Flute	Severity: minor Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisTooManyPowerChassis		
Remedial action: Remove the extra power enclosure.		

Table 27-2240 IK8652391

Alarm	Attributes	Applicable major release
Name: IK8652391 (7680) Type: processingErrorAlarm Package: Img.IK8652391 Raised on class: Img.Flute	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-2241 IK8652392

Alarm	Attributes	Applicable major release
Name: IK8652392 (7681) Type: qualityOfServiceAlarm Package: lmg.IK8652392 Raised on class: lmg.Flute	Severity: minor Specific problem: Enclosure manager degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The Onboard Administrator or other management processor status has been set to degraded. This alarm signifies that either an Onboard Administrator has failed but the other Onboard Administrator is still operating, or one or more management processors is in a non-optimal operating state.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureManagerDegraded		
Remedial action: For C-Class enclosures, replace the Onboard Administrator as soon as possible. For all others please refer to product documenation for possible corrective actions		

Table 27-2242 IK8652397

Alarm	Attributes	Applicable major release
Name: IK8652397 (7682) Type: communicationsAlarm Package: lmg.IK8652397 Raised on class: lmg.LMGMngElement	Severity: minor Specific problem: keying failed Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The server blade e-keying has failed. This alarm signifies that a server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackServerBladeEKeyingFailed		
Remedial action: Reconfigure server blade mezz cards.		

Table 27-2243 IK8652401

Alarm	Attributes	Applicable major release
Name: IK8652401 (7683) Type: communicationsAlarm Package: lmg.IK8652401 Raised on class: lmg.Flute	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-2244 IK8652402

Alarm	Attributes	Applicable major release
Name: IK8652402 (7684) Type: communicationsAlarm Package: Img.IK8652402 Raised on class: Img.Flute	Severity: minor Specific problem: Interconnect degraded Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The interconnect status has been set to degraded. This alarm signifies that a interconnect has degraded.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorDegraded		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-2245 IK8652408

Alarm	Attributes	Applicable major release
Name: IK8652408 (7685) Type: qualityOfServiceAlarm Package: Img.IK8652408 Raised on class: Img.Flute	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2246 IK8652409

Alarm	Attributes	Applicable major release
Name: IK8652409 (7686) Type: processingErrorAlarm Package: Img.IK8652409 Raised on class: Img.Flute	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2247 IK8652410

Alarm	Attributes	Applicable major release
Name: IK8652410 (7687) Type: equipmentAlarm Package: Img.IK8652410 Raised on class: Img.Flute	Severity: minor Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeGrpCapTimeout		
Remedial action: Reset the iLO management processor.		

Table 27-2248 IK8652411

Alarm	Attributes	Applicable major release
Name: IK8652411 (7688) Type: equipmentAlarm Package: Img.IK8652411 Raised on class: Img.Flute	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2249 IK8652427

Alarm	Attributes	Applicable major release
Name: IK8652427 (7689) Type: equipmentAlarm Package: Img.IK8652427 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Generic EAE Minor trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Minor trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMinorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2250 IK8652428

Alarm	Attributes	Applicable major release
Name: IK8652428 (7690) Type: equipmentAlarm Package: Img.IK8652428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2250 IK8652428 (continued)

Alarm	Attributes	Applicable major release
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2251 IK8652429

Alarm	Attributes	Applicable major release
Name: IK8652429 (7691) Type: equipmentAlarm Package: Img.IK8652429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2252 IK8652430

Alarm	Attributes	Applicable major release
Name: IK8652430 (7692) Type: equipmentAlarm Package: Img.IK8652430 Raised on class: Img.Flute	Severity: minor Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMinorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2253 IK8652431

Alarm	Attributes	Applicable major release
Name: IK8652431 (7693) Type: equipmentAlarm Package: Img.IK8652431 Raised on class: Img.Flute	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2254 IK8652432

Alarm	Attributes	Applicable major release
Name: IK8652432 (7694) Type: equipmentAlarm Package: Img.IK8652432 Raised on class: Img.Flute	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2255 IK8652435

Alarm	Attributes	Applicable major release
Name: IK8652435 (7695) Type: equipmentAlarm Package: Img.IK8652435 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Generic WSMAN Minor trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Minor trap\nReason: cpqRackMinorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2256 IK8652436

Alarm	Attributes	Applicable major release
Name: IK8652436 (7696) Type: equipmentAlarm Package: Img.IK8652436 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2257 IK8652437

Alarm	Attributes	Applicable major release
Name: IK8652437 (7697) Type: equipmentAlarm Package: Img.IK8652437 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		

Table 27-2257 IK8652437 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2258 IK8652439

Alarm	Attributes	Applicable major release
Name: IK8652439 (7698) Type: communicationsAlarm Package: Img.IK8652439 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2259 IK8652443

Alarm	Attributes	Applicable major release
Name: IK8652443 (7699) Type: communicationsAlarm Package: Img.IK8652443 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapDeviceConnected		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-2260 IK8652444

Alarm	Attributes	Applicable major release
Name: IK8652444 (7700) Type: communicationsAlarm Package: Img.IK8652444 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG

Table 27-2260 IK8652444 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapConnectionLost		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-2261 IK8652449

Alarm	Attributes	Applicable major release
Name: IK8652449 (7701) Type: environmentalAlarm Package: lmg.IK8652449 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 1 Above Warning Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 1 above warning threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp1AboveWarn		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2262 IK8652450

Alarm	Attributes	Applicable major release
Name: IK8652450 (7702) Type: environmentalAlarm Package: lmg.IK8652450 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 1 Above Maximum Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 1 above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp1AboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2263 IK8652453

Alarm	Attributes	Applicable major release
Name: IK8652453 (7703) Type: environmentalAlarm Package: lmg.IK8652453 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 2 Above Warning Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 2 above warning threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp2AboveWarn		

Table 27-2263 IK8652453 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2264 IK8652454

Alarm	Attributes	Applicable major release
Name: IK8652454 (7704) Type: environmentalAlarm Package: Img.IK8652454 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Temperature 2 Above Maximum Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting temperature 2 above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCTemp2AboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2265 IK8652457

Alarm	Attributes	Applicable major release
Name: IK8652457 (7705) Type: equipmentAlarm Package: Img.IK8652457 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A CMC device is reporting voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCVoltOver		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2266 IK8652460

Alarm	Attributes	Applicable major release
Name: IK8652460 (7706) Type: environmentalAlarm Package: Img.IK8652460 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: CMC Humidity Above Maximum Implicitly cleared: false Default probable cause: humidityUnacceptable	Release: • LR14.3.MG
Description: A CMC device is reporting humidity above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapCMCHmdtOver		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2267 IK8652462

Alarm	Attributes	Applicable major release
Name: IK8652462 (7707) Type: environmentalAlarm Package: lmg.IK8652462 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-2268 IK8652464

Alarm	Attributes	Applicable major release
Name: IK8652464 (7708) Type: equipmentAlarm Package: lmg.IK8652464 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2269 IK8652466

Alarm	Attributes	Applicable major release
Name: IK8652466 (7709) Type: equipmentAlarm Package: lmg.IK8652466 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: CMC Aux 1 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A CMC device has entered an alarm condition for auxiliary input 1.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux1Alarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2270 IK8652468

Alarm	Attributes	Applicable major release
Name: IK8652468 (7710) Type: equipmentAlarm Package: lmg.IK8652468 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2270 IK8652468 (continued)

Alarm	Attributes	Applicable major release
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2271 IK8652489

Alarm	Attributes	Applicable major release
Name: IK8652489 (7711) Type: equipmentAlarm Package: Img.IK8652489 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: UPS Input Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A UPS device is reporting input voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSInputVoltageAboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2272 IK8652490

Alarm	Attributes	Applicable major release
Name: IK8652490 (7712) Type: equipmentAlarm Package: Img.IK8652490 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSInputVoltageNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-2273 IK8652492

Alarm	Attributes	Applicable major release
Name: IK8652492 (7713) Type: equipmentAlarm Package: Img.IK8652492 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: UPS Output Voltage Above Maximum Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A UPS device is reporting output voltage above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSOutputVoltageAboveMax		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2274 IK8652493

Alarm	Attributes	Applicable major release
Name: IK8652493 (7714) Type: equipmentAlarm Package: Img.IK8652493 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOutputVoltageNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-2275 IK8652494

Alarm	Attributes	Applicable major release
Name: IK8652494 (7715) Type: equipmentAlarm Package: Img.IK8652494 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutpu-tOverload		
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-2276 IK8652496

Alarm	Attributes	Applicable major release
Name: IK8652496 (7716) Type: environmentalAlarm Package: Img.IK8652496 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-2277 IK8652499

Alarm	Attributes	Applicable major release
Name: IK8652499 (7717) Type: equipmentAlarm Package: Img.IK8652499 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSBatteryLevelNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-2278 IK8652500

Alarm	Attributes	Applicable major release
Name: IK8652500 (7718) Type: equipmentAlarm Package: Img.IK8652500 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-2279 IK8652502

Alarm	Attributes	Applicable major release
Name: IK8652502 (7719) Type: equipmentAlarm Package: Img.IK8652502 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBuck		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2280 IK8652503

Alarm	Attributes	Applicable major release
Name: IK8652503 (7720) Type: equipmentAlarm Package: Img.IK8652503 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBoost		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2281 IK8652504

Alarm	Attributes	Applicable major release
Name: IK8652504 (7721) Type: equipmentAlarm Package: Img.IK8652504 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnUtilityPower		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-2282 IK8652506

Alarm	Attributes	Applicable major release
Name: IK8652506 (7722) Type: environmentalAlarm Package: Img.IK8652506 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: UPS Temperature High Implicitly cleared: false Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG
Description: A UPS device is reporting temperature above maximum threshold.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRPMTrapUPSTemperatureHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2283 IK8652507

Alarm	Attributes	Applicable major release
Name: IK8652507 (7723) Type: environmentalAlarm Package: Img.IK8652507 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG

Table 27-2283 IK8652507 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSTemperatureNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-2284 IK8652508

Alarm	Attributes	Applicable major release
Name: IK8652508 (7724) Type: equipmentAlarm Package: lmg.IK8652508 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2285 IK8652510

Alarm	Attributes	Applicable major release
Name: IK8652510 (7725) Type: environmentalAlarm Package: lmg.IK8652510 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2286 IK8652512

Alarm	Attributes	Applicable major release
Name: IK8652512 (7726) Type: equipmentAlarm Package: lmg.IK8652512 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestFailed		

Table 27-2286 IK8652512 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2287 IK8652513

Alarm	Attributes	Applicable major release
Name: IK8652513 (7727) Type: equipmentAlarm Package: lmg.IK8652513 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestSucceeded		
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2288 IK8652516

Alarm	Attributes	Applicable major release
Name: IK8652516 (7728) Type: equipmentAlarm Package: lmg.IK8652516 Raised on class: lmg.LMGMngElement	Severity: indeterminate Specific problem: DC Start Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The UPS has been started on battery when AC input power is not present. This alarm is used to record the date and time of this event.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSDCStartOccurred		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2289 IK8652518

Alarm	Attributes	Applicable major release
Name: IK8652518 (7729) Type: equipmentAlarm Package: lmg.IK8652518 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2290 IK8652522

Alarm	Attributes	Applicable major release
Name: IK8652522 (7730) Type: equipmentAlarm Package: Img.IK8652522 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Utility Not Present Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Indicates that the utility input is not present. This differs from alarm #57 in that the detected voltage is zero in this case.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSUtilityNotPresent		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2291 IK8652526

Alarm	Attributes	Applicable major release
Name: IK8652526 (7731) Type: equipmentAlarm Package: Img.IK8652526 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringFault		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2292 IK8652527

Alarm	Attributes	Applicable major release
Name: IK8652527 (7732) Type: equipmentAlarm Package: Img.IK8652527 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2293 IK8652528

Alarm	Attributes	Applicable major release
Name: IK8652528 (7733) Type: equipmentAlarm Package: Img.IK8652528 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-2293 IK8652528 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassOffManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-2294 IK8652529

Alarm	Attributes	Applicable major release
Name: IK8652529 (7734) Type: equipmentAlarm Package: lmg.IK8652529 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassONManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-2295 IK8652531

Alarm	Attributes	Applicable major release
Name: IK8652531 (7735) Type: equipmentAlarm Package: lmg.IK8652531 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-2296 IK8652533

Alarm	Attributes	Applicable major release
Name: IK8652533 (7736) Type: equipmentAlarm Package: lmg.IK8652533 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2296 IK8652533 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInput-OutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-2297 IK8652534

Alarm	Attributes	Applicable major release
Name: IK8652534 (7737) Type: environmentalAlarm Package: lmg.IK8652534 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTem-peratureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-2298 IK8652536

Alarm	Attributes	Applicable major release
Name: IK8652536 (7738) Type: equipmentAlarm Package: lmg.IK8652536 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassO-nAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-2299 IK8652538

Alarm	Attributes	Applicable major release
Name: IK8652538 (7739) Type: equipmentAlarm Package: lmg.IK8652538 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-2299 IK8652538 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMtrapUPSOutputoutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-2300 IK8652539

Alarm	Attributes	Applicable major release
Name: IK8652539 (7740) Type: equipmentAlarm Package: lmg.IK8652539 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-2301 IK8652541

Alarm	Attributes	Applicable major release
Name: IK8652541 (7741) Type: environmentalAlarm Package: lmg.IK8652541 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-2302 IK8652543

Alarm	Attributes	Applicable major release
Name: IK8652543 (7742) Type: equipmentAlarm Package: lmg.IK8652543 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2302 IK8652543 (continued)

Alarm	Attributes	Applicable major release
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2303 IK8652545

Alarm	Attributes	Applicable major release
Name: IK8652545 (7743) Type: equipmentAlarm Package: Img.IK8652545 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSEPOInitiated		
Remedial action: Perform the following steps to clear the alarm: 1. Turn the UPS on to reapply power to attached equipment.		

Table 27-2304 IK8652546

Alarm	Attributes	Applicable major release
Name: IK8652546 (9345) Type: equipmentAlarm Package: Img.IK8652546 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2305 IK8652548

Alarm	Attributes	Applicable major release
Name: IK8652548 (7744) Type: environmentalAlarm Package: Img.IK8652548 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		

Table 27-2305 IK8652548 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2306 IK8652550

Alarm	Attributes	Applicable major release
Name: IK8652550 (7745) Type: environmentalAlarm Package: Img.IK8652550 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If the problem persists, contact NOKIA customer support.		

Table 27-2307 IK8652552

Alarm	Attributes	Applicable major release
Name: IK8652552 (7746) Type: processingErrorAlarm Package: Img.IK8652552 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-2308 IK8652554

Alarm	Attributes	Applicable major release
Name: IK8652554 (7747) Type: equipmentAlarm Package: Img.IK8652554 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-2309 IK8652556

Alarm	Attributes	Applicable major release
Name: IK8652556 (7748) Type: equipmentAlarm Package: Img.IK8652556 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-2310 IK8652559

Alarm	Attributes	Applicable major release
Name: IK8652559 (7749) Type: equipmentAlarm Package: Img.IK8652559 Raised on class: Img.Flute	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-2311 IK8652560

Alarm	Attributes	Applicable major release
Name: IK8652560 (7750) Type: equipmentAlarm Package: Img.IK8652560 Raised on class: Img.Flute	Severity: warning Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A warning alarm has occurred.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqPMTrapWarning		
Remedial action: Check the Trap Details for more information.		

Table 27-2312 IK8652585

Alarm	Attributes	Applicable major release
Name: IK8652585 (7751) Type: processingErrorAlarm Package: Img.IK8652585 Raised on class: Img.Flute	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomizationError	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-2313 IK8652586

Alarm	Attributes	Applicable major release
Name: IK8652586 (7752) Type: equipmentAlarm Package: Img.IK8652586 Raised on class: Img.Flute	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-2314 IK8652590

Alarm	Attributes	Applicable major release
Name: IK8652590 (7753) Type: environmentalAlarm Package: Img.IK8652590 Raised on class: Img.Flute	Severity: minor Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3LibraryDoorOpen		
Remedial action: Close the door on the tape library.		

Table 27-2315 IK8652606

Alarm	Attributes	Applicable major release
Name: IK8652606 (7754) Type: equipmentAlarm Package: Img.IK8652606 Raised on class: Img.Flute	Severity: warning Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHoodRemoved		
Remedial action: Replace the cover (hood), ensure the system's cover is properly installed. Verify the system is in working order.		

Table 27-2316 IK8652608

Alarm	Attributes	Applicable major release
Name: IK8652608 (7755) Type: environmentalAlarm Package: Img.IK8652608 Raised on class: Img.Flute	Severity: minor Specific problem: Monitor Condition Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits for the monitor indicated by the cpqSiMonitorIndex. The monitor's condition is degraded due to the internal temperature exceeding normal operating limits. The monitor is still useable, but action should be taken to return the condition to OK.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionDegraded		
Remedial action: Physically check for obstructions to air flow around the monitor. Check the thermostat in the room that the system occupies. Allow the monitor to cool by turning off the monitor for 5 minutes then turn the monitor back on. After the monitor cools, another alarm indicating an improving condition, such as Monitor OK, will be issued.		

Table 27-2317 IK8652609

Alarm	Attributes	Applicable major release
Name: IK8652609 (7756) Type: processingErrorAlarm Package: Img.IK8652609 Raised on class: Img.Flute	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2318 IK8652610

Alarm	Attributes	Applicable major release
Name: IK8652610 (7757) Type: processingErrorAlarm Package: Img.IK8652610 Raised on class: Img.Flute	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2319 IK8652612

Alarm	Attributes	Applicable major release
Name: IK8652612 (7758) Type: processingErrorAlarm Package: Img.IK8652612 Raised on class: Img.Flute	Severity: warning Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiMemConfigChange		
Remedial action: You may want to verify a valid reason for a memory configuration to have occurred. If system issuing the alert is a Desktop running NT, the memory configuration change information is also logged in the NT System Log.		

Table 27-2320 IK8652615

Alarm	Attributes	Applicable major release
Name: IK8652615 (7759) Type: equipmentAlarm Package: Img.IK8652615 Raised on class: Img.Flute	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-2321 IK8652616

Alarm	Attributes	Applicable major release
Name: IK8652616 (7760) Type: environmentalAlarm Package: Img.IK8652616 Raised on class: Img.Flute	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-2322 IK8652617

Alarm	Attributes	Applicable major release
Name: IK8652617 (7761) Type: environmentalAlarm Package: Img.IK8652617 Raised on class: Img.Flute	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-2323 IK8652618

Alarm	Attributes	Applicable major release
Name: IK8652618 (7762) Type: environmentalAlarm Package: Img.IK8652618 Raised on class: Img.Flute	Severity: warning Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryCalibrationError		
Remedial action: Run the Power Conservation Utility. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-2324 IK8652619

Alarm	Attributes	Applicable major release
Name: IK8652619 (7763) Type: processingErrorAlarm Package: Img.IK8652619 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Server Reset Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Reset Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server reset.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerReset		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2325 IK8652620

Alarm	Attributes	Applicable major release
Name: IK8652620 (7764) Type: equipmentAlarm Package: Img.IK8652620 Raised on class: Img.Flute	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-2326 IK8652621

Alarm	Attributes	Applicable major release
Name: IK8652621 (7765) Type: securityServiceOrMechanismViolation Package: Img.IK8652621 Raised on class: Img.LMGMngElement	Severity: warning Specific problem: Out Unauthorized Login Attempts Implicitly cleared: false Default probable cause: unauthorizedAccessAttempt	Release: • LR14.3.MG

Table 27-2326 IK8652621 (continued)

Alarm	Attributes	Applicable major release
Description: Remote Insight/ Integrated Lights-Out Unauthorized Login Attempts. The Remote Insight/ Integrated Lights-Out firmware has detected unauthorized login attempts.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2UnauthorizedLoginAttempts		
Remedial action: Check the iLO log for more information on the login failure.		

Table 27-2327 IK8652622

Alarm	Attributes	Applicable major release
Name: IK8652622 (7766) Type: environmentalAlarm Package: lmg.IK8652622 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-2328 IK8652628

Alarm	Attributes	Applicable major release
Name: IK8652628 (7767) Type: equipmentAlarm Package: lmg.IK8652628 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-2329 IK8652630

Alarm	Attributes	Applicable major release
Name: IK8652630 (7768) Type: processingErrorAlarm Package: lmg.IK8652630 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Security override engaged Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Security Override Engaged. The Remote Insight/ Integrated Lights-Out firmware has detected the security override jumper has been toggled to the engaged position.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2SecurityOverrideEngaged		

Table 27-2329 IK8652630 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2330 IK8652631

Alarm	Attributes	Applicable major release
Name: IK8652631 (7769) Type: processingErrorAlarm Package: lmg.IK8652631 Raised on class: lmg.LMGMngElement	Severity: warning Specific problem: Security override disengaged Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Security Override Disengaged. The Remote Insight/ Integrated Lights-Out firmware has detected the security override jumper has been toggled to the disengaged position.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2SecurityOverrideDisengaged		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2331 IK8652632

Alarm	Attributes	Applicable major release
Name: IK8652632 (7770) Type: processingErrorAlarm Package: lmg.IK8652632 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2332 IK8652633

Alarm	Attributes	Applicable major release
Name: IK8652633 (7771) Type: communicationsAlarm Package: lmg.IK8652633 Raised on class: lmg.Flute	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-2333 IK8652636

Alarm	Attributes	Applicable major release
Name: IK8652636 (9346) Type: equipmentAlarm Package: Img.IK8652636 Raised on class: Img.Flute	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2334 IK8652647

Alarm	Attributes	Applicable major release
Name: IK8652647 (7772) Type: qualityOfServiceAlarm Package: Img.IK8652647 Raised on class: Img.Flute	Severity: minor Specific problem: PC Card Thermal Degraded Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for safe operations thereby causing degraded operations. This alarm will be sent when cpqSePCCardStatus transitions from Normal (1) to Thermal Degraded (2). The manufacturer and product information strings as well as the slot number for the degraded PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalDegraded		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2335 IK8652648

Alarm	Attributes	Applicable major release
Name: IK8652648 (7773) Type: qualityOfServiceAlarm Package: Img.IK8652648 Raised on class: Img.Flute	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2336 IK8652657

Alarm	Attributes	Applicable major release
Name: IK8652657 (7774) Type: environmentalAlarm Package: lmg.IK8652657 Raised on class: lmg.Flute	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2337 IK8652658

Alarm	Attributes	Applicable major release
Name: IK8652658 (7775) Type: environmentalAlarm Package: lmg.IK8652658 Raised on class: lmg.Flute	Severity: minor Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system.\nReason: cpqSsTempDegraded		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2338 IK8652661

Alarm	Attributes	Applicable major release
Name: IK8652661 (7776) Type: equipmentAlarm Package: lmg.IK8652661 Raised on class: lmg.Flute	Severity: minor Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system.\nReason: cpqSsSidePanelRemoved		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2339 IK8652662

Alarm	Attributes	Applicable major release
Name: IK8652662 (7777) Type: equipmentAlarm Package: Img.IK8652662 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A storage system power supply status has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSsPwrSupplyDegraded		
Remedial action: check the storage system power supply		

Table 27-2340 IK8652664

Alarm	Attributes	Applicable major release
Name: IK8652664 (7778) Type: environmentalAlarm Package: Img.IK8652664 Raised on class: Img.Flute	Severity: warning Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempFailed		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-2341 IK8652665

Alarm	Attributes	Applicable major release
Name: IK8652665 (7779) Type: environmentalAlarm Package: Img.IK8652665 Raised on class: Img.Flute	Severity: warning Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempDegraded		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-2342 IK8652668

Alarm	Attributes	Applicable major release
Name: IK8652668 (7780) Type: equipmentAlarm Package: Img.IK8652668 Raised on class: Img.Flute	Severity: warning Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3SidePanelRemoved		
Remedial action: Replace the storage system side panel.		

Table 27-2343 IK8652669

Alarm	Attributes	Applicable major release
Name: IK8652669 (7781) Type: equipmentAlarm Package: Img.IK8652669 Raised on class: Img.LMGMngElement	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A storage system power supply status has been set to degraded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSs3PwrSupplyDegraded		
Remedial action: check the storage system power supply		

Table 27-2344 IK8652670

Alarm	Attributes	Applicable major release
Name: IK8652670 (7782) Type: equipmentAlarm Package: Img.IK8652670 Raised on class: Img.Flute	Severity: warning Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A storage system power supply status has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs4PwrSupplyDegraded		
Remedial action: Take action to restore power or replace any failed storage system power supply.		

Table 27-2345 IK8652695

Alarm	Attributes	Applicable major release
Name: IK8652695 (7783) Type: equipmentAlarm Package: Img.IK8652695 Raised on class: Img.Flute	Severity: minor Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMeRisingAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2346 IK8652697

Alarm	Attributes	Applicable major release
Name: IK8652697 (7784) Type: equipmentAlarm Package: Img.IK8652697 Raised on class: Img.Flute	Severity: warning Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMe2RisingAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2347 IK8652699

Alarm	Attributes	Applicable major release
Name: IK8652699 (7785) Type: equipmentAlarm Package: Img.IK8652699 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMeRisingAlarm-Extended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2348 IK8652700

Alarm	Attributes	Applicable major release
Name: IK8652700 (7786) Type: equipmentAlarm Package: Img.IK8652700 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Falling Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Falling Threshold passed. An alarm entry has crossed its falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeFallingAlarmExtended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2349 IK8652701

Alarm	Attributes	Applicable major release
Name: IK8652701 (7787) Type: equipmentAlarm Package: Img.IK8652701 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Critical Rising Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Critical Rising Threshold passed. An alarm entry has crossed its Critical rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeCriticalRisingAlarmExtended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2350 IK8652702

Alarm	Attributes	Applicable major release
Name: IK8652702 (7788) Type: equipmentAlarm Package: Img.IK8652702 Raised on class: Img.LMGMngElement	Severity: indeterminate Specific problem: Critical Falling Threshold Passed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Critical Falling Threshold passed. An alarm entry has crossed its Critical falling threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm to be cleared by the operator at the management system.\nReason: cpqMeCriticalFallingAlarmExtended		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2351 IK8652748

Alarm	Attributes	Applicable major release
Name: IK8652748 (7789) Type: equipmentAlarm Package: lmg.IK8652748 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: fluteModuleAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Alarm notification\nAlarm is cleared by the system.\nReason: fluteModuleAlarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2352 IK8654762

Alarm	Attributes	Applicable major release
Name: IK8654762 (7790) Type: communicationsAlarm Package: lmg.IK8654762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2353 IK8657456

Alarm	Attributes	Applicable major release
Name: IK8657456 (9347) Type: environmentalAlarm Package: lmg.IK8657456 Raised on class: lmg.Flute	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The temperature at rack sensor 1 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp1		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2354 IK8657457

Alarm	Attributes	Applicable major release
Name: IK8657457 (9348) Type: environmentalAlarm Package: lmg.IK8657457 Raised on class: lmg.Flute	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The temperature at rack sensor 2 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp2		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2355 IK8657458

Alarm	Attributes	Applicable major release
Name: IK8657458 (9349) Type: environmentalAlarm Package: lmg.IK8657458 Raised on class: lmg.Flute	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The status of Fan 1 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan1		
Remedial action: Refer to Trap Details for more information.		

Table 27-2356 IK8657459

Alarm	Attributes	Applicable major release
Name: IK8657459 (9350) Type: environmentalAlarm Package: lmg.IK8657459 Raised on class: lmg.Flute	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The status of Fan 2 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan2		
Remedial action: Refer to Trap Details for more information.		

Table 27-2357 IK8657460

Alarm	Attributes	Applicable major release
Name: IK8657460 (9351) Type: equipmentAlarm Package: lmg.IK8657460 Raised on class: lmg.Flute	Severity: warning Specific problem: Voltage-alarm Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG

Table 27-2357 IK8657460 (continued)

Alarm	Attributes	Applicable major release
Description: The AC voltage of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmVoltage		
Remedial action: Check the incoming power source and ensure all cables are inserted correctly.		

Table 27-2358 IK8657461

Alarm	Attributes	Applicable major release
Name: IK8657461 (9352) Type: environmentalAlarm Package: Img.IK8657461 Raised on class: Img.Flute	Severity: warning Specific problem: Humidity-alarm Implicitly cleared: true Default probable cause: humidityUnacceptable	Release: • LR15.1.MG • LR16.1.MG
Description: The humidity of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmHumidity		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-2359 IK8657462

Alarm	Attributes	Applicable major release
Name: IK8657462 (9353) Type: environmentalAlarm Package: Img.IK8657462 Raised on class: Img.Flute	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #1).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput1		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2360 IK8657463

Alarm	Attributes	Applicable major release
Name: IK8657463 (9354) Type: environmentalAlarm Package: Img.IK8657463 Raised on class: Img.Flute	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #2).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput2		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2361 IK8657464

Alarm	Attributes	Applicable major release
Name: IK8657464 (9355) Type: environmentalAlarm Package: Img.IK8657464 Raised on class: Img.Flute	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #3).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput3		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2362 IK8657465

Alarm	Attributes	Applicable major release
Name: IK8657465 (9356) Type: environmentalAlarm Package: Img.IK8657465 Raised on class: Img.Flute	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG • LR16.1.MG
Description: The door or sidepanel of the rack has been opened (access point #4).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput4		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2363 IK8657466

Alarm	Attributes	Applicable major release
Name: IK8657466 (9357) Type: processingErrorAlarm Package: Img.IK8657466 Raised on class: Img.Flute	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: Rack door lock #1 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2364 IK8657467

Alarm	Attributes	Applicable major release
Name: IK8657467 (9358) Type: processingErrorAlarm Package: Img.IK8657467 Raised on class: Img.Flute	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: Rack door lock #2 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-2365 IK8657468

Alarm	Attributes	Applicable major release
Name: IK8657468 (9359) Type: environmentalAlarm Package: Img.IK8657468 Raised on class: Img.Flute	Severity: warning Specific problem: Smoke-alarm Implicitly cleared: true Default probable cause: smoke	Release: • LR15.1.MG • LR16.1.MG
Description: The rack smoke detector has detected smoke.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmSmoke		
Remedial action: Investigate rack for an over temperature condition and refer to Trap Details for more information.		

Table 27-2366 IK8657469

Alarm	Attributes	Applicable major release
Name: IK8657469 (9360) Type: environmentalAlarm Package: Img.IK8657469 Raised on class: Img.Flute	Severity: warning Specific problem: Shock-alarm Implicitly cleared: true Default probable cause: excessiveVibration	Release: • LR15.1.MG • LR16.1.MG
Description: The rack shock detector has detected a vibration to the rack.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmShock		
Remedial action: Investigate rack.		

Table 27-2367 IK8657474

Alarm	Attributes	Applicable major release
Name: IK8657474 (9361) Type: processingErrorAlarm Package: Img.IK8657474 Raised on class: Img.Flute	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: The rack door locking device #1 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-2368 IK8657475

Alarm	Attributes	Applicable major release
Name: IK8657475 (9362) Type: processingErrorAlarm Package: Img.IK8657475 Raised on class: Img.Flute	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG • LR16.1.MG
Description: The rack door locking device #2 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-2369 IK8657477

Alarm	Attributes	Applicable major release
Name: IK8657477 (9363) Type: processingErrorAlarm Package: Img.IK8657477 Raised on class: Img.Flute	Severity: warning Specific problem: Corrected - uncorrectable Memory Errors - Replace Memory Module Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG • LR16.1.MG
Description: Corrected - uncorrected Memory Errors Detected The errors have been corrected, but the memory module should be replaced. Value 0 for CPU means memory is not Processor based\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqHe5CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module.		

Table 27-2370 IK8657478

Alarm	Attributes	Applicable major release
Name: IK8657478 (9364) Type: communicationsAlarm Package: lmg.IK8657478 Raised on class: lmg.Flute	Severity: warning Specific problem: NIC Virus-like Activity Detected Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent when the Virus Throttle Filter Driver detects virus like activity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNicVirusLikeActivityDetected		
Remedial action: The system reporting this trap requires immediate attention.		

Table 27-2371 IK8657479

Alarm	Attributes	Applicable major release
Name: IK8657479 (9365) Type: communicationsAlarm Package: lmg.IK8657479 Raised on class: lmg.Flute	Severity: minor Specific problem: Server Blade e-keying failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: The server blade e-keying has failed. This alarm signifies that a server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeEKeyingFailed		
Remedial action: Reconfigure server blade mezz cards.		

Table 27-2372 IK8657481

Alarm	Attributes	Applicable major release
Name: IK8657481 (10770) Type: equipmentAlarm Package: lmg.IK8657481 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.		
Remedial action: No action is required.		

Table 27-2373 IK8657482

Alarm	Attributes	Applicable major release
Name: IK8657482 (10771) Type: equipmentAlarm Package: Img.IK8657482 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.		
Remedial action: No action is required.		

Table 27-2374 IK8657483

Alarm	Attributes	Applicable major release
Name: IK8657483 (10772) Type: equipmentAlarm Package: Img.IK8657483 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.		
Remedial action: No action is required.		

Table 27-2375 IK8657484

Alarm	Attributes	Applicable major release
Name: IK8657484 (10773) Type: equipmentAlarm Package: Img.IK8657484 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.		
Remedial action: No action is required.		

Table 27-2376 IK8657485

Alarm	Attributes	Applicable major release
Name: IK8657485 (10774) Type: equipmentAlarm Package: Img.IK8657485 Raised on class: Img.Flute	Severity: indeterminate Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.		
Remedial action: No action is required.		

Table 27-2377 IK8657486

Alarm	Attributes	Applicable major release
Name: IK8657486 (10775) Type: equipmentAlarm Package: Img.IK8657486 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-2378 IK8657487

Alarm	Attributes	Applicable major release
Name: IK8657487 (10776) Type: equipmentAlarm Package: Img.IK8657487 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-2379 IK8657488

Alarm	Attributes	Applicable major release
Name: IK8657488 (10777) Type: equipmentAlarm Package: Img.IK8657488 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-2380 IK8657489

Alarm	Attributes	Applicable major release
Name: IK8657489 (10778) Type: equipmentAlarm Package: Img.IK8657489 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.		

Table 27-2380 IK8657489 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2381 IK8657490

Alarm	Attributes	Applicable major release
Name: IK8657490 (10779) Type: equipmentAlarm Package: lmg.IK8657490 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-2382 IK8657491

Alarm	Attributes	Applicable major release
Name: IK8657491 (10780) Type: equipmentAlarm Package: lmg.IK8657491 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-2383 IK8657500

Alarm	Attributes	Applicable major release
Name: IK8657500 (10781) Type: equipmentAlarm Package: lmg.IK8657500 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes degraded.		
Remedial action: No action is required.		

Table 27-2384 IK8657501

Alarm	Attributes	Applicable major release
Name: IK8657501 (10782) Type: equipmentAlarm Package: Img.IK8657501 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes failed.		
Remedial action: No action is required.		

Table 27-2385 IK8657502

Alarm	Attributes	Applicable major release
Name: IK8657502 (10783) Type: equipmentAlarm Package: Img.IK8657502 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes degraded.		
Remedial action: No action is required.		

Table 27-2386 IK8657503

Alarm	Attributes	Applicable major release
Name: IK8657503 (10784) Type: equipmentAlarm Package: Img.IK8657503 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes failed.		
Remedial action: No action is required.		

Table 27-2387 IK8657504

Alarm	Attributes	Applicable major release
Name: IK8657504 (10785) Type: equipmentAlarm Package: Img.IK8657504 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes degraded.		

Table 27-2387 IK8657504 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2388 IK8657505

Alarm	Attributes	Applicable major release
Name: IK8657505 (10786) Type: equipmentAlarm Package: lmg.IK8657505 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes failed.		
Remedial action: No action is required.		

Table 27-2389 IK8657508

Alarm	Attributes	Applicable major release
Name: IK8657508 (10787) Type: equipmentAlarm Package: lmg.IK8657508 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2390 IK8657509

Alarm	Attributes	Applicable major release
Name: IK8657509 (10788) Type: equipmentAlarm Package: lmg.IK8657509 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-2391 IK8657510

Alarm	Attributes	Applicable major release
Name: IK8657510 (10789) Type: equipmentAlarm Package: Img.IK8657510 Raised on class: Img.Flute	Severity: indeterminate Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: External Array Redundant Controller Active. This event signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.		
Remedial action: No action is required.		

Table 27-2392 IK8657511

Alarm	Attributes	Applicable major release
Name: IK8657511 (10790) Type: equipmentAlarm Package: Img.IK8657511 Raised on class: Img.Flute	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2393 IK8657512

Alarm	Attributes	Applicable major release
Name: IK8657512 (10791) Type: equipmentAlarm Package: Img.IK8657512 Raised on class: Img.Flute	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-2394 IK8657513

Alarm	Attributes	Applicable major release
Name: IK8657513 (10792) Type: equipmentAlarm Package: lmg.IK8657513 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log		
Remedial action: No action is required.		

Table 27-2395 IK8657514

Alarm	Attributes	Applicable major release
Name: IK8657514 (10793) Type: equipmentAlarm Package: lmg.IK8657514 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.		
Remedial action: No action is required.		

Table 27-2396 IK8657515

Alarm	Attributes	Applicable major release
Name: IK8657515 (10794) Type: equipmentAlarm Package: lmg.IK8657515 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-2397 IK8657516

Alarm	Attributes	Applicable major release
Name: IK8657516 (10795) Type: equipmentAlarm Package: lmg.IK8657516 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-2398 IK8657517

Alarm	Attributes	Applicable major release
Name: IK8657517 (10796) Type: equipmentAlarm Package: Img.IK8657517 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-2399 IK8657518

Alarm	Attributes	Applicable major release
Name: IK8657518 (10797) Type: equipmentAlarm Package: Img.IK8657518 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-2400 IK8657519

Alarm	Attributes	Applicable major release
Name: IK8657519 (10798) Type: equipmentAlarm Package: Img.IK8657519 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.		
Remedial action: No action is required.		

Table 27-2401 IK8657520

Alarm	Attributes	Applicable major release
Name: IK8657520 (10799) Type: equipmentAlarm Package: Img.IK8657520 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.		

Table 27-2401 IK8657520 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2402 IK8657521

Alarm	Attributes	Applicable major release
Name: IK8657521 (10800) Type: equipmentAlarm Package: lmg.IK8657521 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.		
Remedial action: No action is required.		

Table 27-2403 IK8657522

Alarm	Attributes	Applicable major release
Name: IK8657522 (10801) Type: equipmentAlarm Package: lmg.IK8657522 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.		
Remedial action: No action is required.		

Table 27-2404 IK8657523

Alarm	Attributes	Applicable major release
Name: IK8657523 (10802) Type: equipmentAlarm Package: lmg.IK8657523 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.		
Remedial action: No action is required.		

Table 27-2405 IK8657524

Alarm	Attributes	Applicable major release
Name: IK8657524 (10803) Type: equipmentAlarm Package: Img.IK8657524 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.		
Remedial action: No action is required.		

Table 27-2406 IK8657525

Alarm	Attributes	Applicable major release
Name: IK8657525 (10804) Type: equipmentAlarm Package: Img.IK8657525 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.		
Remedial action: No action is required.		

Table 27-2407 IK8657526

Alarm	Attributes	Applicable major release
Name: IK8657526 (10805) Type: equipmentAlarm Package: Img.IK8657526 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.		
Remedial action: No action is required.		

Table 27-2408 IK8657527

Alarm	Attributes	Applicable major release
Name: IK8657527 (10806) Type: equipmentAlarm Package: lmg.IK8657527 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.		
Remedial action: No action is required.		

Table 27-2409 IK8657528

Alarm	Attributes	Applicable major release
Name: IK8657528 (10807) Type: equipmentAlarm Package: lmg.IK8657528 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-2410 IK8657529

Alarm	Attributes	Applicable major release
Name: IK8657529 (10808) Type: equipmentAlarm Package: lmg.IK8657529 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-2411 IK8657530

Alarm	Attributes	Applicable major release
Name: IK8657530 (10809) Type: equipmentAlarm Package: Img.IK8657530 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.		
Remedial action: No action is required.		

Table 27-2412 IK8657531

Alarm	Attributes	Applicable major release
Name: IK8657531 (10810) Type: equipmentAlarm Package: Img.IK8657531 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the configured redundant NIC becomes the active NIC.		
Remedial action: No action is required.		

Table 27-2413 IK8657532

Alarm	Attributes	Applicable major release
Name: IK8657532 (10811) Type: equipmentAlarm Package: Img.IK8657532 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.MG
Description: This event is a send to the user to notify him of a Critical Software Update.		
Remedial action: No action is required.		

Table 27-2414 IK8657533

Alarm	Attributes	Applicable major release
Name: IK8657533 (10812) Type: equipmentAlarm Package: Img.IK8657533 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-2414 IK8657533 (continued)

Alarm	Attributes	Applicable major release
Description: Controller Active. This event signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.		
Remedial action: No action is required.		

Table 27-2415 IK8657534

Alarm	Attributes	Applicable major release
Name: IK8657534 (10813) Type: equipmentAlarm Package: lmg.IK8657534 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2416 IK8657535

Alarm	Attributes	Applicable major release
Name: IK8657535 (10814) Type: equipmentAlarm Package: lmg.IK8657535 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Accelerator Board Bad Data. This event signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2417 IK8657536

Alarm	Attributes	Applicable major release
Name: IK8657536 (10815) Type: equipmentAlarm Package: lmg.IK8657536 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the array accelerator cache board.		
Remedial action: No action is required.		

Table 27-2418 IK8657537

Alarm	Attributes	Applicable major release
Name: IK8657537 (10816) Type: equipmentAlarm Package: Img.IK8657537 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2419 IK8657538

Alarm	Attributes	Applicable major release
Name: IK8657538 (10817) Type: equipmentAlarm Package: Img.IK8657538 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2420 IK8657539

Alarm	Attributes	Applicable major release
Name: IK8657539 (10818) Type: equipmentAlarm Package: Img.IK8657539 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Cache Module Board Bad Data. This event signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-2421 IK8657540

Alarm	Attributes	Applicable major release
Name: IK8657540 (10819) Type: equipmentAlarm Package: Img.IK8657540 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG

Table 27-2421 IK8657540 (continued)

Alarm	Attributes	Applicable major release
Description: Cache Module Board Backup Power Source Failed. This event signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-2422 IK8657541

Alarm	Attributes	Applicable major release
Name: IK8657541 (10820) Type: equipmentAlarm Package: Img.IK8657541 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-2423 IK8657542

Alarm	Attributes	Applicable major release
Name: IK8657542 (10821) Type: equipmentAlarm Package: Img.IK8657542 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-2424 IK8657543

Alarm	Attributes	Applicable major release
Name: IK8657543 (10822) Type: equipmentAlarm Package: Img.IK8657543 Raised on class: Img.Flute	Severity: indeterminate Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.		
Remedial action: No action is required.		

Table 27-2425 IK8657545

Alarm	Attributes	Applicable major release
Name: IK8657545 (10823) Type: equipmentAlarm Package: lmg.IK8657545 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.		
Remedial action: No action is required.		

Table 27-2426 IK8657546

Alarm	Attributes	Applicable major release
Name: IK8657546 (10824) Type: equipmentAlarm Package: lmg.IK8657546 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to failed. This event signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-2427 IK8657547

Alarm	Attributes	Applicable major release
Name: IK8657547 (10825) Type: equipmentAlarm Package: lmg.IK8657547 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to degraded. This event signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-2428 IK8657548

Alarm	Attributes	Applicable major release
Name: IK8657548 (10826) Type: equipmentAlarm Package: Img.IK8657548 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to failed. This event signifies that a power supply has failed.		
Remedial action: No action is required.		

Table 27-2429 IK8657549

Alarm	Attributes	Applicable major release
Name: IK8657549 (10827) Type: equipmentAlarm Package: Img.IK8657549 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to degraded. This event signifies that a power supply has degraded.		
Remedial action: No action is required.		

Table 27-2430 IK8657550

Alarm	Attributes	Applicable major release
Name: IK8657550 (10828) Type: equipmentAlarm Package: Img.IK8657550 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem is no longer in a redundant state.		
Remedial action: No action is required.		

Table 27-2431 IK8657551

Alarm	Attributes	Applicable major release
Name: IK8657551 (10829) Type: equipmentAlarm Package: Img.IK8657551 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power supply detected an input line voltage problem.		

Table 27-2431 IK8657551 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2432 IK8657552

Alarm	Attributes	Applicable major release
Name: IK8657552 (10830) Type: equipmentAlarm Package: Img.IK8657552 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem overload condition.		
Remedial action: No action is required.		

Table 27-2433 IK8657553

Alarm	Attributes	Applicable major release
Name: IK8657553 (10831) Type: equipmentAlarm Package: Img.IK8657553 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.		
Remedial action: No action is required.		

Table 27-2434 IK8657554

Alarm	Attributes	Applicable major release
Name: IK8657554 (10832) Type: equipmentAlarm Package: Img.IK8657554 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.		
Remedial action: No action is required.		

Table 27-2435 IK8657555

Alarm	Attributes	Applicable major release
Name: IK8657555 (10833) Type: equipmentAlarm Package: Img.IK8657555 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.		
Remedial action: No action is required.		

Table 27-2436 IK8657556

Alarm	Attributes	Applicable major release
Name: IK8657556 (10834) Type: equipmentAlarm Package: Img.IK8657556 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-2437 IK8657557

Alarm	Attributes	Applicable major release
Name: IK8657557 (10835) Type: equipmentAlarm Package: Img.IK8657557 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-2438 IK8657558

Alarm	Attributes	Applicable major release
Name: IK8657558 (10836) Type: equipmentAlarm Package: Img.IK8657558 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Fuse open. The fuse has been tripped.		

Table 27-2438 IK8657558 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2439 IK8657559

Alarm	Attributes	Applicable major release
Name: IK8657559 (10837) Type: equipmentAlarm Package: Img.IK8657559 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.		
Remedial action: No action is required.		

Table 27-2440 IK8657560

Alarm	Attributes	Applicable major release
Name: IK8657560 (10838) Type: equipmentAlarm Package: Img.IK8657560 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.		
Remedial action: No action is required.		

Table 27-2441 IK8657561

Alarm	Attributes	Applicable major release
Name: IK8657561 (10839) Type: equipmentAlarm Package: Img.IK8657561 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.		
Remedial action: No action is required.		

Table 27-2442 IK8657562

Alarm	Attributes	Applicable major release
Name: IK8657562 (10840) Type: equipmentAlarm Package: Img.IK8657562 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.		
Remedial action: No action is required.		

Table 27-2443 IK8657563

Alarm	Attributes	Applicable major release
Name: IK8657563 (10841) Type: equipmentAlarm Package: Img.IK8657563 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.		
Remedial action: No action is required.		

Table 27-2444 IK8657564

Alarm	Attributes	Applicable major release
Name: IK8657564 (10842) Type: equipmentAlarm Package: Img.IK8657564 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.		
Remedial action: No action is required.		

Table 27-2445 IK8657565

Alarm	Attributes	Applicable major release
Name: IK8657565 (10843) Type: equipmentAlarm Package: Img.IK8657565 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG

Table 27-2445 IK8657565 (continued)

Alarm	Attributes	Applicable major release
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.		
Remedial action: No action is required.		

Table 27-2446 IK8657566

Alarm	Attributes	Applicable major release
Name: IK8657566 (10844) Type: equipmentAlarm Package: Img.IK8657566 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.		
Remedial action: No action is required.		

Table 27-2447 IK8657567

Alarm	Attributes	Applicable major release
Name: IK8657567 (10845) Type: equipmentAlarm Package: Img.IK8657567 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper		
Remedial action: No action is required.		

Table 27-2448 IK8657568

Alarm	Attributes	Applicable major release
Name: IK8657568 (10846) Type: equipmentAlarm Package: Img.IK8657568 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.		
Remedial action: No action is required.		

Table 27-2449 IK8657569

Alarm	Attributes	Applicable major release
Name: IK8657569 (10847) Type: equipmentAlarm Package: Img.IK8657569 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.		
Remedial action: No action is required.		

Table 27-2450 IK8657570

Alarm	Attributes	Applicable major release
Name: IK8657570 (10848) Type: equipmentAlarm Package: Img.IK8657570 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.		
Remedial action: No action is required.		

Table 27-2451 IK8657571

Alarm	Attributes	Applicable major release
Name: IK8657571 (10849) Type: equipmentAlarm Package: Img.IK8657571 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.		
Remedial action: No action is required.		

Table 27-2452 IK8657572

Alarm	Attributes	Applicable major release
Name: IK8657572 (10850) Type: equipmentAlarm Package: Img.IK8657572 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Generic WSMAN Major trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-2452 IK8657572 (continued)

Alarm	Attributes	Applicable major release
Description: WSMAN Major trap		
Remedial action: No action is required.		

Table 27-2453 IK8657573

Alarm	Attributes	Applicable major release
Name: IK8657573 (10851) Type: equipmentAlarm Package: Img.IK8657573 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Generic WSMAN Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Critical trap		
Remedial action: No action is required.		

Table 27-2454 IK8657574

Alarm	Attributes	Applicable major release
Name: IK8657574 (10852) Type: equipmentAlarm Package: Img.IK8657574 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-2455 IK8657575

Alarm	Attributes	Applicable major release
Name: IK8657575 (10853) Type: equipmentAlarm Package: Img.IK8657575 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-2456 IK8657576

Alarm	Attributes	Applicable major release
Name: IK8657576 (10854) Type: equipmentAlarm Package: Img.IK8657576 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.		
Remedial action: No action is required.		

Table 27-2457 IK8657577

Alarm	Attributes	Applicable major release
Name: IK8657577 (10855) Type: equipmentAlarm Package: Img.IK8657577 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-2458 IK8657578

Alarm	Attributes	Applicable major release
Name: IK8657578 (10856) Type: equipmentAlarm Package: Img.IK8657578 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.		
Remedial action: No action is required.		

Table 27-2459 IK8657579

Alarm	Attributes	Applicable major release
Name: IK8657579 (10857) Type: equipmentAlarm Package: Img.IK8657579 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-2460 IK8657580

Alarm	Attributes	Applicable major release
Name: IK8657580 (10858) Type: equipmentAlarm Package: Img.IK8657580 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.		
Remedial action: No action is required.		

Table 27-2461 IK8657581

Alarm	Attributes	Applicable major release
Name: IK8657581 (10859) Type: equipmentAlarm Package: Img.IK8657581 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.		
Remedial action: No action is required.		

Table 27-2462 IK8657582

Alarm	Attributes	Applicable major release
Name: IK8657582 (10860) Type: equipmentAlarm Package: Img.IK8657582 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-2463 IK8657583

Alarm	Attributes	Applicable major release
Name: IK8657583 (10861) Type: equipmentAlarm Package: Img.IK8657583 Raised on class: Img.Flute	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.		

Table 27-2463 IK8657583 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2464 IK8657584

Alarm	Attributes	Applicable major release
Name: IK8657584 (10862) Type: equipmentAlarm Package: lmg.IK8657584 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-2465 IK8657585

Alarm	Attributes	Applicable major release
Name: IK8657585 (10863) Type: equipmentAlarm Package: lmg.IK8657585 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-2466 IK8657586

Alarm	Attributes	Applicable major release
Name: IK8657586 (10864) Type: equipmentAlarm Package: lmg.IK8657586 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-2467 IK8657587

Alarm	Attributes	Applicable major release
Name: IK8657587 (10865) Type: equipmentAlarm Package: Img.IK8657587 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-2468 IK8657588

Alarm	Attributes	Applicable major release
Name: IK8657588 (10866) Type: equipmentAlarm Package: Img.IK8657588 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-2469 IK8657589

Alarm	Attributes	Applicable major release
Name: IK8657589 (10867) Type: equipmentAlarm Package: Img.IK8657589 Raised on class: Img.Flute	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-2470 IK8657590

Alarm	Attributes	Applicable major release
Name: IK8657590 (10868) Type: equipmentAlarm Package: Img.IK8657590 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-2471 IK8657591

Alarm	Attributes	Applicable major release
Name: IK8657591 (10869) Type: equipmentAlarm Package: Img.IK8657591 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.		
Remedial action: No action is required.		

Table 27-2472 IK8657592

Alarm	Attributes	Applicable major release
Name: IK8657592 (10870) Type: equipmentAlarm Package: Img.IK8657592 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-2473 IK8657593

Alarm	Attributes	Applicable major release
Name: IK8657593 (10871) Type: equipmentAlarm Package: Img.IK8657593 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-2474 IK8657594

Alarm	Attributes	Applicable major release
Name: IK8657594 (10872) Type: equipmentAlarm Package: Img.IK8657594 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-2474 IK8657594 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-2475 IK8657595

Alarm	Attributes	Applicable major release
Name: IK8657595 (10873) Type: equipmentAlarm Package: lmg.IK8657595 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.		
Remedial action: No action is required.		

Table 27-2476 IK8657596

Alarm	Attributes	Applicable major release
Name: IK8657596 (10874) Type: equipmentAlarm Package: lmg.IK8657596 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.		
Remedial action: No action is required.		

Table 27-2477 IK8657597

Alarm	Attributes	Applicable major release
Name: IK8657597 (10875) Type: equipmentAlarm Package: lmg.IK8657597 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.		
Remedial action: No action is required.		

Table 27-2478 IK8657598

Alarm	Attributes	Applicable major release
Name: IK8657598 (10876) Type: equipmentAlarm Package: Img.IK8657598 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.		
Remedial action: No action is required.		

Table 27-2479 IK8657599

Alarm	Attributes	Applicable major release
Name: IK8657599 (10877) Type: equipmentAlarm Package: Img.IK8657599 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.		
Remedial action: No action is required.		

Table 27-2480 IK8657600

Alarm	Attributes	Applicable major release
Name: IK8657600 (10878) Type: equipmentAlarm Package: Img.IK8657600 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.		
Remedial action: No action is required.		

Table 27-2481 IK8657601

Alarm	Attributes	Applicable major release
Name: IK8657601 (10879) Type: equipmentAlarm Package: Img.IK8657601 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.		

Table 27-2481 IK8657601 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2482 IK8657602

Alarm	Attributes	Applicable major release
Name: IK8657602 (10880) Type: equipmentAlarm Package: Img.IK8657602 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.		
Remedial action: No action is required.		

Table 27-2483 IK8657603

Alarm	Attributes	Applicable major release
Name: IK8657603 (10881) Type: equipmentAlarm Package: Img.IK8657603 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.		
Remedial action: No action is required.		

Table 27-2484 IK8657604

Alarm	Attributes	Applicable major release
Name: IK8657604 (10882) Type: equipmentAlarm Package: Img.IK8657604 Raised on class: Img.Flute	Severity: indeterminate Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.		
Remedial action: No action is required.		

Table 27-2485 IK8657605

Alarm	Attributes	Applicable major release
Name: IK8657605 (10883) Type: equipmentAlarm Package: lmg.IK8657605 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.		
Remedial action: No action is required.		

Table 27-2486 IK8657606

Alarm	Attributes	Applicable major release
Name: IK8657606 (10884) Type: equipmentAlarm Package: lmg.IK8657606 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.		
Remedial action: No action is required.		

Table 27-2487 IK8657607

Alarm	Attributes	Applicable major release
Name: IK8657607 (10885) Type: equipmentAlarm Package: lmg.IK8657607 Raised on class: lmg.Flute	Severity: indeterminate Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A storage system power supply status has been set to degraded.		
Remedial action: No action is required.		

Table 27-2488 IK8690000

Alarm	Attributes	Applicable major release
Name: IK8690000 (9366) Type: processingErrorAlarm Package: lmg.IK8690000 Raised on class: lmg.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG

Table 27-2488 IK8690000 (continued)

Alarm	Attributes	Applicable major release
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2489 IK8690001

Alarm	Attributes	Applicable major release
Name: IK8690001 (9367) Type: processingErrorAlarm Package: Img.IK8690001 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2490 IK8690002

Alarm	Attributes	Applicable major release
Name: IK8690002 (9368) Type: processingErrorAlarm Package: Img.IK8690002 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2491 IK8690003

Alarm	Attributes	Applicable major release
Name: IK8690003 (9369) Type: processingErrorAlarm Package: Img.IK8690003 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2492 IK8690004

Alarm	Attributes	Applicable major release
Name: IK8690004 (9370) Type: processingErrorAlarm Package: lmg.IK8690004 Raised on class: lmg.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2493 IK8690005

Alarm	Attributes	Applicable major release
Name: IK8690005 (9371) Type: processingErrorAlarm Package: lmg.IK8690005 Raised on class: lmg.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2494 IK8690006

Alarm	Attributes	Applicable major release
Name: IK8690006 (9372) Type: processingErrorAlarm Package: lmg.IK8690006 Raised on class: lmg.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2495 IK8690007

Alarm	Attributes	Applicable major release
Name: IK8690007 (9373) Type: processingErrorAlarm Package: lmg.IK8690007 Raised on class: lmg.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2496 IK8690008

Alarm	Attributes	Applicable major release
Name: IK8690008 (9374) Type: processingErrorAlarm Package: Img.IK8690008 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2497 IK8690009

Alarm	Attributes	Applicable major release
Name: IK8690009 (9375) Type: processingErrorAlarm Package: Img.IK8690009 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2498 IK8690010

Alarm	Attributes	Applicable major release
Name: IK8690010 (9376) Type: processingErrorAlarm Package: Img.IK8690010 Raised on class: Img.Flute	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2499 IK8690011

Alarm	Attributes	Applicable major release
Name: IK8690011 (9377) Type: processingErrorAlarm Package: Img.IK8690011 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2500 IK8690012

Alarm	Attributes	Applicable major release
Name: IK8690012 (9378) Type: processingErrorAlarm Package: lmg.IK8690012 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2501 IK8690013

Alarm	Attributes	Applicable major release
Name: IK8690013 (9379) Type: processingErrorAlarm Package: lmg.IK8690013 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2502 IK8690014

Alarm	Attributes	Applicable major release
Name: IK8690014 (9380) Type: processingErrorAlarm Package: lmg.IK8690014 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2503 IK8690015

Alarm	Attributes	Applicable major release
Name: IK8690015 (9381) Type: processingErrorAlarm Package: lmg.IK8690015 Raised on class: lmg.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2504 IK8690016

Alarm	Attributes	Applicable major release
Name: IK8690016 (9382) Type: processingErrorAlarm Package: Img.IK8690016 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2505 IK8690017

Alarm	Attributes	Applicable major release
Name: IK8690017 (9383) Type: processingErrorAlarm Package: Img.IK8690017 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2506 IK8690018

Alarm	Attributes	Applicable major release
Name: IK8690018 (9384) Type: processingErrorAlarm Package: Img.IK8690018 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2507 IK8690019

Alarm	Attributes	Applicable major release
Name: IK8690019 (9385) Type: processingErrorAlarm Package: Img.IK8690019 Raised on class: Img.FilePrepare	Severity: warning Specific problem: Provision Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: This is a spare for future use		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2508 IK8705835

Alarm	Attributes	Applicable major release
Name: IK8705835 (7791) Type: equipmentAlarm Package: lmg.IK8705835 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: emergencyTrap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A user-defined alarm indicating an extremely urgent situation, usually indicating that the system has failed and is shutting down.\nAlarm to be cleared by the operator at the management system.\nReason: emergencyTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2509 IK8705836

Alarm	Attributes	Applicable major release
Name: IK8705836 (7792) Type: processingErrorAlarm Package: lmg.IK8705836 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: alertTrap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: A user-defined alarm indicating a condition that should be corrected immediately, such as a failed disk.\nAlarm to be cleared by the operator at the management system.\nReason: alertTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2510 IK8705837

Alarm	Attributes	Applicable major release
Name: IK8705837 (7793) Type: equipmentAlarm Package: lmg.IK8705837 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: criticalTrap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A user-defined alarm indicating a critical condition, such as a hard device error.\nAlarm to be cleared by the operator at the management system.\nReason: criticalTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2511 IK8705843

Alarm	Attributes	Applicable major release
Name: IK8705843 (7794) Type: processingErrorAlarm Package: lmg.IK8705843 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: diskFailedShutdown Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG

Table 27-2511 IK8705843 (continued)

Alarm	Attributes	Applicable major release
Description: System is shutting down because the system has been running in degraded mode for 24 hours. The alarm includes a string describing the failed disk.\nAlarm is cleared by the system.\nReason: diskFailedShutdown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2512 IK8705844

Alarm	Attributes	Applicable major release
Name: IK8705844 (7795) Type: processingErrorAlarm Package: lmg.IK8705844 Raised on class: lmg.FRU	Severity: critical Specific problem: One or more disks failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One or more disks failed. The alarm includes a string describing the failed disk(s).\nAlarm is cleared by the system.\nReason: diskFailed		
Remedial action: Replace the disk device.		

Table 27-2513 IK8705846

Alarm	Attributes	Applicable major release
Name: IK8705846 (7796) Type: environmentalAlarm Package: lmg.IK8705846 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: fanFailureShutdown Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: Critical chassis or cpu fans have failed and the system is shutting down.\nAlarm to be cleared by the operator at the management system.\nReason: fanFailureShutdown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2514 IK8705849

Alarm	Attributes	Applicable major release
Name: IK8705849 (7797) Type: equipmentAlarm Package: lmg.IK8705849 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: powerSupplyFailureShutdown Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Critical power supplies or power rails failed and the system is shutting down.\nAlarm to be cleared by the operator at the management system.\nReason: powerSupplyFailureShutdown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2515 IK8705850

Alarm	Attributes	Applicable major release
Name: IK8705850 (7798) Type: equipmentAlarm Package: lmg.IK8705850 Raised on class: lmg.FRU	Severity: critical Specific problem: One or more redundant power supplies failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One or more redundant power supplies failed. Include in the alarm a string describing the failed power supply(ies).\nAlarm is cleared by the system.\nReason: powerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2516 IK8705853

Alarm	Attributes	Applicable major release
Name: IK8705853 (7799) Type: equipmentAlarm Package: lmg.IK8705853 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: CPU utilization exceeds 90% Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: CPU utilization exceeds 90%. This alarm is not enabled by default. To enable this alarm set the registry entry options.monitor.cpu.enable to on. Note that as the threshold for this alarm is checked once a minute it is possible to receive multiple instances of this alarm in a short time.\nAlarm is cleared by the system.\nReason: cpuTooBusy		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2517 IK8705855

Alarm	Attributes	Applicable major release
Name: IK8705855 (7800) Type: environmentalAlarm Package: lmg.IK8705855 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The NVRAM battery is fully discharged Implicitly cleared: false Default probable cause: batteryDischarging	Release: • LR14.3.MG
Description: The NVRAM battery is fully discharged.\nAlarm to be cleared by the operator at the management system.\nReason: nvramBatteryDischarged		
Remedial action: Check the NVRAM battery		

Table 27-2518 IK8705856

Alarm	Attributes	Applicable major release
Name: IK8705856 (7801) Type: environmentalAlarm Package: lmg.IK8705856 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: The charge in the NVRAM battery is low Implicitly cleared: false Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG
Description: The charge in the NVRAM battery is low.\nAlarm to be cleared by the operator at the management system.\nReason: nvramBatteryLow		
Remedial action: check the NVRAM battery		

Table 27-2519 IK8705862

Alarm	Attributes	Applicable major release
Name: IK8705862 (9386) Type: processingErrorAlarm Package: lmg.IK8705862 Raised on class: lmg.FRU	Severity: critical Specific problem: At least one volume is more than 95% full Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: At least one volume is more than 95% full. The string sent with the alarm gives the name of the volume or volumes which exceed the volumeFull or volumeNearlyFull thresholds\nAlarm is cleared by the system.\nReason: volumeNearlyFull		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2520 IK8705865

Alarm	Attributes	Applicable major release
Name: IK8705865 (7802) Type: environmentalAlarm Package: lmg.IK8705865 Raised on class: lmg.FRU	Severity: critical Specific problem: System temperature is too high to continue operating Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: System temperature is too high to continue operating. The system is shutting down.\nAlarm is cleared by the system.\nReason: overTempShutdown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2521 IK8705868

Alarm	Attributes	Applicable major release
Name: IK8705868 (9387) Type: processingErrorAlarm Package: lmg.IK8705868 Raised on class: lmg.FRU	Severity: major Specific problem: shelfFault Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR15.1.MG • LR16.1.MG
Description: A disk storage shelf reported a fault, probably due to a problem with drive placement, fans, power, or temperature.\nAlarm is cleared by the system.\nReason: shelfFault		
Remedial action: Check drive placement, fans, power, and temperature		

Table 27-2522 IK8705870

Alarm	Attributes	Applicable major release
Name: IK8705870 (7803) Type: processingErrorAlarm Package: lmg.IK8705870 Raised on class: lmg.FRU	Severity: critical Specific problem: globalStatusNonRecoverable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The appliance's overall status changed to 'nonRecoverable', indicating a problem so severe that the appliance is shutting down.\nAlarm is cleared by the system.\nReason: globalStatusNonRecoverable		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2523 IK8705871

Alarm	Attributes	Applicable major release
Name: IK8705871 (7804) Type: processingErrorAlarm Package: lmg.IK8705871 Raised on class: lmg.FRU	Severity: critical Specific problem: globalStatusCritical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The appliance's overall status changed to 'critical', indicating a problem that needs immediate attention.\nAlarm is cleared by the system.\nReason: globalStatusCritical		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2524 IK8705872

Alarm	Attributes	Applicable major release
Name: IK8705872 (7805) Type: processingErrorAlarm Package: lmg.IK8705872 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: globalStatusNonCritical Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG

Table 27-2524 IK8705872 (continued)

Alarm	Attributes	Applicable major release
Description: The appliance's overall status changed to 'nonCritical', indicating a problem that needs attention.\nAlarm to be cleared by the operator at the management system.\nReason: globalStatusNonCritical		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2525 IK8705881

Alarm	Attributes	Applicable major release
Name: IK8705881 (7806) Type: environmentalAlarm Package: lmg.IK8705881 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: UPS: Shutting down now: Time left on battery is exhausted Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: UPS: Shutting down now: Time left on battery is exhausted.\nAlarm to be cleared by the operator at the management system.\nReason: upsShuttingDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2526 IK8705882

Alarm	Attributes	Applicable major release
Name: IK8705882 (7807) Type: environmentalAlarm Package: lmg.IK8705882 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: UPS: Warning: Time left on battery is getting critical Implicitly cleared: false Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG
Description: UPS: Warning: Time left on battery is getting critical.\nAlarm to be cleared by the operator at the management system.\nReason: upsBatteryWarning		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2527 IK8705884

Alarm	Attributes	Applicable major release
Name: IK8705884 (7808) Type: processingErrorAlarm Package: lmg.IK8705884 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: appEmergency Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The application encountered an extremely urgent situation and requires an immediate response.\nAlarm to be cleared by the operator at the management system.\nReason: appEmergency		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2528 IK8705885

Alarm	Attributes	Applicable major release
Name: IK8705885 (7809) Type: processingErrorAlarm Package: lmg.IK8705885 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: appAlert Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The application is in a condition that should be corrected immediately.\nAlarm to be cleared by the operator at the management system.\nReason: appAlert		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2529 IK8705900

Alarm	Attributes	Applicable major release
Name: IK8705900 (7810) Type: processingErrorAlarm Package: lmg.IK8705900 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: eccMasked Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: Memory ECC: High frequency of ECC errors\nAlarm to be cleared by the operator at the management system.\nReason: eccMasked		
Remedial action: check Memory ECC		

Table 27-2530 IK8705902

Alarm	Attributes	Applicable major release
Name: IK8705902 (7811) Type: communicationsAlarm Package: lmg.IK8705902 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: ftpdMaxConnNotice Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Ftp daemon: number of connections hits maximum number\nAlarm to be cleared by the operator at the management system.\nReason: ftpdMaxConnNotice		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2531 IK8705907

Alarm	Attributes	Applicable major release
Name: IK8705907 (7812) Type: equipmentAlarm Package: lmg.IK8705907 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: vifPrimaryLinkFailed Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2531 IK8705907 (continued)

Alarm	Attributes	Applicable major release
Description: Vif: The primary Interface on a Single mode vif has failed\nAlarm to be cleared by the operator at the management system.\nReason: vifPrimaryLinkFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2532 IK8705908

Alarm	Attributes	Applicable major release
Name: IK8705908 (7813) Type: communicationsAlarm Package: lmg.IK8705908 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: vifAllLinksFailed Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Vif: All the links of the vif have failed\nAlarm to be cleared by the operator at the management system.\nReason: vifAllLinksFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2533 IK8705916

Alarm	Attributes	Applicable major release
Name: IK8705916 (7814) Type: processingErrorAlarm Package: lmg.IK8705916 Raised on class: lmg.FRU	Severity: critical Specific problem: volumeRestrictedByMirrorBigIo Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A volume that experienced a medium error during reconstruction is restricted and marked wafl-inconsistent, but starting wafliron has failed. This alarm is issued to alert operator that a volume is not accessible and wafliron must be started to allow access to it.\nAlarm is cleared by the system.\nReason: volumeRestrictedByMirrorBigIo		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2534 IK8705921

Alarm	Attributes	Applicable major release
Name: IK8705921 (7815) Type: equipmentAlarm Package: lmg.IK8705921 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: rmcCardMissingCables Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Remote Management Controller card is missing its internal cable, or LAN cable or power supply cable. The alarm includes a string specifying the missing component.\nAlarm to be cleared by the operator at the management system.\nReason: rmcCardMissingCables		

Table 27-2534 IK8705921 (continued)

Alarm	Attributes	Applicable major release
Remedial action: check Remote Management Controller card and its internal cable		

Table 27-2535 IK8705933

Alarm	Attributes	Applicable major release
Name: IK8705933 (9388) Type: equipmentAlarm Package: lmg.IK8705933 Raised on class: lmg.FRU	Severity: major Specific problem: snapmirrorSyncFailed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: Synchronous SnapMirror failed and went into asynchronous mode.\nAlarm is cleared by the system.\nReason: snapmirrorSyncFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2536 IK8705935

Alarm	Attributes	Applicable major release
Name: IK8705935 (7816) Type: processingErrorAlarm Package: lmg.IK8705935 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The chassis temperature is extreme Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The chassis temperature is extreme. The appliance has initiated a shutdown to protect itself. The operating environment should be monitored and corrected before restarting the appliance.\nAlarm to be cleared by the operator at the management system.\nReason: chassisTemperatureShutdown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2537 IK8705939

Alarm	Attributes	Applicable major release
Name: IK8705939 (7817) Type: environmentalAlarm Package: lmg.IK8705939 Raised on class: lmg.FRU	Severity: critical Specific problem: One or more CPU fans have stopped Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One or more CPU fans have stopped. The appliance has initiated a shutdown to protect itself. A new motherboard may be required to correct the fan. Contact customer support for direction.\nAlarm is cleared by the system.\nReason: chassisCPUFanStopped		
Remedial action: Check the motherboard		

Table 27-2538 IK8705940

Alarm	Attributes	Applicable major release
Name: IK8705940 (9998) Type: environmentalAlarm Package: lmg.IK8705940 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A CPU fan is spinning too slowly Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: A CPU fan is spinning too slowly. A new motherboard may be required to correct the fan. Contact customer support for direction.\nAlarm is cleared by the system.\nReason: chassisCPUFanSlow		
Remedial action: Check the motherboard		

Table 27-2539 IK8705942

Alarm	Attributes	Applicable major release
Name: IK8705942 (7818) Type: equipmentAlarm Package: lmg.IK8705942 Raised on class: lmg.FRU	Severity: critical Specific problem: Multiple chassis power supplies failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Multiple chassis power supplies failed.\nAlarm is cleared by the system.\nReason: chassisPowerSuppliesFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2540 IK8705943

Alarm	Attributes	Applicable major release
Name: IK8705943 (7819) Type: equipmentAlarm Package: lmg.IK8705943 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: One or more chassis power supplies are degraded Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more chassis power supplies are degraded. A description of the degraded state has been logged to the console and message log file.\nAlarm to be cleared by the operator at the management system.\nReason: chassisPowerSupplyDegraded		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2541 IK8705944

Alarm	Attributes	Applicable major release
Name: IK8705944 (7820) Type: equipmentAlarm Package: lmg.IK8705944 Raised on class: lmg.FRU	Severity: critical Specific problem: One chassis power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One chassis power supply failed.\nAlarm is cleared by the system.\nReason: chassisPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2542 IK8705946

Alarm	Attributes	Applicable major release
Name: IK8705946 (9389) Type: equipmentAlarm Package: lmg.IK8705946 Raised on class: lmg.FRU	Severity: major Specific problem: One or more chassis power supplies are off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: One or more chassis power supplies are off.\nAlarm is cleared by the system.\nReason: chassisPowerSupplyOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2543 IK8705957

Alarm	Attributes	Applicable major release
Name: IK8705957 (7821) Type: communicationsAlarm Package: lmg.IK8705957 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: prefDCDisconnect Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: All connections to domain controllers in the preferred domain controllers list have been lost.\nAlarm to be cleared by the operator at the management system.\nReason: prefDCDisconnect		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2544 IK8705963

Alarm	Attributes	Applicable major release
Name: IK8705963 (7822) Type: equipmentAlarm Package: lmg.IK8705963 Raised on class: lmg.FRU	Severity: critical Specific problem: shelfSESElectronicsFailed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-2544 IK8705963 (continued)

Alarm	Attributes	Applicable major release
Description: One or more of the enclosure services devices in a disk shelf has failed. Some shelf designs combine the enclosure monitoring hardware function into the module that provides the storage interface to the shelf. A failure in the enclosure monitoring section of these combined modules does not necessarily indicate a failure in disk or loop or bus operation, which may be able to continue.\nAlarm is cleared by the system.\nReason: shelfSESElectronicsFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2545 IK8705965

Alarm	Attributes	Applicable major release
Name: IK8705965 (7823) Type: equipmentAlarm Package: lmg.IK8705965 Raised on class: lmg.FRU	Severity: major Specific problem: shelfIFModuleFailed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: One or more of the storage interface modules in a disk shelf has failed. Some shelf designs combine the enclosure monitoring hardware function into the module that operates the fibre channel loop or SCSI in the shelf. This failure is of the storage interface itself, not a failure of the enclosure monitoring, which may be able to continue. This failure may make one or more disks in the shelf or in the loop or bus unavailable.\nAlarm is cleared by the system.\nReason: shelfIFModuleFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2546 IK8705971

Alarm	Attributes	Applicable major release
Name: IK8705971 (7824) Type: equipmentAlarm Package: lmg.IK8705971 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Unit is removed from the system Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Power Supply Unit is removed from the system. System will be shutdown in x minutes if it is not put back.\nAlarm to be cleared by the operator at the management system.\nReason: chassisPSRemovedxMinShutdown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2547 IK8705973

Alarm	Attributes	Applicable major release
Name: IK8705973 (7825) Type: environmentalAlarm Package: lmg.IK8705973 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Multiple chassis fan failure Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG

Table 27-2547 IK8705973 (continued)

Alarm	Attributes	Applicable major release
Description: Multiple chassis fan failure. System will shut down in a few minutes if not corrected.\nAlarm to be cleared by the operator at the management system.\nReason: chassisFanFailxMinShutdown		
Remedial action: Check the chassis fan		

Table 27-2548 IK8705974

Alarm	Attributes	Applicable major release
Name: IK8705974 (7826) Type: equipmentAlarm Package: lmg.IK8705974 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: chassisPSUwrongInput Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Power Supply Unit (PSU) in the system is connected to an incompatible external power source.\nAlarm to be cleared by the operator at the management system.\nReason: chassisPSUwrongInput		
Remedial action: Change the power source being used or replace the PSU with one that matches the current power source.		

Table 27-2549 IK8705975

Alarm	Attributes	Applicable major release
Name: IK8705975 (7827) Type: environmentalAlarm Package: lmg.IK8705975 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Multiple power supply fans failure Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: Multiple power supply fans failure. System will shut down in a few minutes if not corrected.\nAlarm to be cleared by the operator at the management system.\nReason: powerSupplyFanFailxMinShutdown		
Remedial action: Check power supply fans		

Table 27-2550 IK8705976

Alarm	Attributes	Applicable major release
Name: IK8705976 (7828) Type: equipmentAlarm Package: lmg.IK8705976 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: system remote management detected a system down event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-2550 IK8705976 (continued)

Alarm	Attributes	Applicable major release
Description: system remote management detected a system down event. The alarm includes a string describing the specific event which triggered the trap. The string is structured in the following form: Remote Management Event: type="{system_down|system_up|test|keep_alive}, severity={alert|warning|notice|normal|debug|info}, event={post_error|watchdog_reset|power_loss|abnormal_reboot}, key=value An example of a complete message would be: Remote Management Event: type=system_down, severity=alert, event=watchdog_reset, ss=16bytes Additional key=value items may, in the future, be appended to this message. The events that would generate this alarm would be: post_error: Fatal POST error on boot power_loss: Loss of power to system abnormal_reboot: I2_watchdog_reset\nAlarm to be cleared by the operator at the management system.\nReason: remoteSystemMgtAlert"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2551 IK8705977

Alarm	Attributes	Applicable major release
Name: IK8705977 (7829) Type: equipmentAlarm Package: lmg.IK8705977 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: system remote management detected a system down event Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: system remote management detected a system down event. The alarm includes a string describing the specific event which triggered the trap. The string is structured in the following form: Remote Management Event: type="{system_down|system_up|test|keep_alive}, severity={alert|warning|notice|normal|debug|info}, event={loss-of-heartbeat}, key=value An example of a complete message would be: Remote Management Event: type=system_down, severity=warning, event=loss_of_heartbeat, ss=16bytes Additional key=value items may, in the future, be appended to this message. The events that would generate this alarm would be: loss_of_heartbeat: Loss of heartbeat to the RLM.\nAlarm to be cleared by the operator at the management system.\nReason: remoteSystemMgmtWarning"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2552 IK8705978

Alarm	Attributes	Applicable major release
Name: IK8705978 (7830) Type: equipmentAlarm Package: lmg.IK8705978 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: system remote management detected a system down event Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: system remote management detected a system down event. The alarm includes a string describing the specific event which triggered the trap. The string is structured in the following form: Remote Management Event: type="{system_down|system_up|test|keep_alive}, severity={alert|warning|notice|normal|debug|info}, event={power_off_via_rlm,power_cycle_via_rlm,reset_via_rlm}, key=value An example of a complete message would be: Remote Management Event: type=system_down, severity=notice, event=power_off_via_rlm, ss=16bytes Additional key=value items may, in the future, be appended to this message. The events that would generate this alarm would be: power_off_via_rlm: This indicates system power off power_cycle_via_rlm: This indicates system power cycle reset_via_rlm: This indicates system reset.\nAlarm to be cleared by the operator at the management system.\nReason: remoteSystemMgmtNotification"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2553 IK8705984

Alarm	Attributes	Applicable major release
Name: IK8705984 (7831) Type: equipmentAlarm Package: Img.IK8705984 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: driveDisableErr Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A drive has been disabled by the shelf module due to hardware errors. If it is the only drive in the shelf that is disabled, replace the drive.\nAlarm to be cleared by the operator at the management system.\nReason: driveDisableErr		
Remedial action: Replace the failing drive		

Table 27-2554 IK8706001

Alarm	Attributes	Applicable major release
Name: IK8706001 (7832) Type: equipmentAlarm Package: Img.IK8706001 Raised on class: Img.LMGMngElement	Severity: major Specific problem: rebootAbnormal Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: System rebooted abnormally after any of the following events: event =" watchdog reset, agent watchdog reset, panic, power-glitch.\nAlarm to be cleared by the operator at the management system.\nReason: rebootAbnormal"		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2555 IK8706007

Alarm	Attributes	Applicable major release
Name: IK8706007 (7833) Type: communicationsAlarm Package: Img.IK8706007 Raised on class: Img.LMGMngElement	Severity: major Specific problem: scsibladeOutOfQuorum Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: The node has lost connectivity with the other nodes in the cluster. Both fcp and iscsi traffic have been disabled on this node. The corrective action is to reboot the node, and if the node is waiting for giveback then perform a giveback.\nAlarm to be cleared by the operator at the management system.\nReason: scsibladeOutOfQuorum		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2556 IK8707446

Alarm	Attributes	Applicable major release
Name: IK8707446 (9390) Type: processingErrorAlarm Package: lmg.IK8707446 Raised on class: lmg.FRU	Severity: major Specific problem: QoS dynamic memory has reached its limit Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG • LR16.1.MG
Description: QoS dynamic memory has reached its limit. Some QoS features may operate in a limited capacity.\nAlarm is cleared by the system.\nReason: qosMonitorMemoryMaxed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2557 IK8707451

Alarm	Attributes	Applicable major release
Name: IK8707451 (9391) Type: securityServiceOrMechanismViolation Package: lmg.IK8707451 Raised on class: lmg.FRU	Severity: major Specific problem: cifsAuthQueueBuildUp Implicitly cleared: true Default probable cause: authenticationFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The authentication queue is building up due to a dead or slow CIFS domain controller connection. This OID is not available from the Cluster management interfaces.\nAlarm is cleared by the system.\nReason: cifsAuthQueueBuildUp		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2558 IK8750982

Alarm	Attributes	Applicable major release
Name: IK8750982 (7834) Type: equipmentAlarm Package: lmg.IK8750982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-2559 IK8750984

Alarm	Attributes	Applicable major release
Name: IK8750984 (7835) Type: processingErrorAlarm Package: lmg.IK8750984 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-2560 IK8750986

Alarm	Attributes	Applicable major release
Name: IK8750986 (7836) Type: equipmentAlarm Package: lmg.IK8750986 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-2561 IK8751008

Alarm	Attributes	Applicable major release
Name: IK8751008 (7837) Type: equipmentAlarm Package: lmg.IK8751008 Raised on class: lmg.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2562 IK8751010

Alarm	Attributes	Applicable major release
Name: IK8751010 (7838) Type: equipmentAlarm Package: Img.IK8751010 Raised on class: Img.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2563 IK8751013

Alarm	Attributes	Applicable major release
Name: IK8751013 (7839) Type: equipmentAlarm Package: Img.IK8751013 Raised on class: Img.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-2564 IK8751018

Alarm	Attributes	Applicable major release
Name: IK8751018 (7840) Type: processingErrorAlarm Package: Img.IK8751018 Raised on class: Img.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2565 IK8751023

Alarm	Attributes	Applicable major release
Name: IK8751023 (7841) Type: processingErrorAlarm Package: Img.IK8751023 Raised on class: Img.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2566 IK8751030

Alarm	Attributes	Applicable major release
Name: IK8751030 (7842) Type: equipmentAlarm Package: Img.IK8751030 Raised on class: Img.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2567 IK8751033

Alarm	Attributes	Applicable major release
Name: IK8751033 (7843) Type: equipmentAlarm Package: Img.IK8751033 Raised on class: Img.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-2568 IK8751037

Alarm	Attributes	Applicable major release
Name: IK8751037 (7844) Type: equipmentAlarm Package: lmg.IK8751037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2569 IK8751040

Alarm	Attributes	Applicable major release
Name: IK8751040 (7845) Type: environmentalAlarm Package: lmg.IK8751040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriti-calTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-2570 IK8751060

Alarm	Attributes	Applicable major release
Name: IK8751060 (7846) Type: environmentalAlarm Package: lmg.IK8751060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2571 IK8751073

Alarm	Attributes	Applicable major release
Name: IK8751073 (7847) Type: environmentalAlarm Package: lmg.IK8751073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2572 IK8751091

Alarm	Attributes	Applicable major release
Name: IK8751091 (9392) Type: environmentalAlarm Package: lmg.IK8751091 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2573 IK8751098

Alarm	Attributes	Applicable major release
Name: IK8751098 (7848) Type: equipmentAlarm Package: lmg.IK8751098 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2574 IK8751102

Alarm	Attributes	Applicable major release
Name: IK8751102 (7849) Type: environmentalAlarm Package: Img.IK8751102 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2575 IK8751105

Alarm	Attributes	Applicable major release
Name: IK8751105 (7850) Type: environmentalAlarm Package: Img.IK8751105 Raised on class: Img.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2576 IK8751112

Alarm	Attributes	Applicable major release
Name: IK8751112 (7851) Type: equipmentAlarm Package: Img.IK8751112 Raised on class: Img.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2577 IK8751116

Alarm	Attributes	Applicable major release
Name: IK8751116 (7852) Type: equipmentAlarm Package: lmg.IK8751116 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2578 IK8751121

Alarm	Attributes	Applicable major release
Name: IK8751121 (7853) Type: environmentalAlarm Package: lmg.IK8751121 Raised on class: lmg.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2579 IK8751125

Alarm	Attributes	Applicable major release
Name: IK8751125 (7854) Type: environmentalAlarm Package: lmg.IK8751125 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2580 IK8751129

Alarm	Attributes	Applicable major release
Name: IK8751129 (7855) Type: equipmentAlarm Package: lmg.IK8751129 Raised on class: lmg.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-2580 IK8751129 (continued)

Alarm	Attributes	Applicable major release
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-2581 IK8751135

Alarm	Attributes	Applicable major release
Name: IK8751135 (7856) Type: equipmentAlarm Package: lmg.IK8751135 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2582 IK8751144

Alarm	Attributes	Applicable major release
Name: IK8751144 (7857) Type: processingErrorAlarm Package: lmg.IK8751144 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-2583 IK8751148

Alarm	Attributes	Applicable major release
Name: IK8751148 (7858) Type: equipmentAlarm Package: lmg.IK8751148 Raised on class: lmg.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-2584 IK8751152

Alarm	Attributes	Applicable major release
Name: IK8751152 (7859) Type: processingErrorAlarm Package: lmg.IK8751152 Raised on class: lmg.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-2585 IK8751154

Alarm	Attributes	Applicable major release
Name: IK8751154 (7860) Type: equipmentAlarm Package: lmg.IK8751154 Raised on class: lmg.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-2586 IK8751156

Alarm	Attributes	Applicable major release
Name: IK8751156 (7861) Type: processingErrorAlarm Package: lmg.IK8751156 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2587 IK8751158

Alarm	Attributes	Applicable major release
Name: IK8751158 (7862) Type: processingErrorAlarm Package: lmg.IK8751158 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2588 IK8751160

Alarm	Attributes	Applicable major release
Name: IK8751160 (9393) Type: communicationsAlarm Package: lmg.IK8751160 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2589 IK8751163

Alarm	Attributes	Applicable major release
Name: IK8751163 (7863) Type: communicationsAlarm Package: lmg.IK8751163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2590 IK8751172

Alarm	Attributes	Applicable major release
Name: IK8751172 (7864) Type: qualityOfServiceAlarm Package: lmg.IK8751172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2591 IK8752265

Alarm	Attributes	Applicable major release
Name: IK8752265 (7865) Type: environmentalAlarm Package: lmg.IK8752265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2592 IK8752272

Alarm	Attributes	Applicable major release
Name: IK8752272 (7866) Type: environmentalAlarm Package: lmg.IK8752272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2593 IK8752279

Alarm	Attributes	Applicable major release
Name: IK8752279 (7867) Type: environmentalAlarm Package: lmg.IK8752279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2594 IK8752291

Alarm	Attributes	Applicable major release
Name: IK8752291 (7868) Type: equipmentAlarm Package: lmg.IK8752291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2595 IK8752292

Alarm	Attributes	Applicable major release
Name: IK8752292 (7869) Type: environmentalAlarm Package: lmg.IK8752292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2596 IK8752295

Alarm	Attributes	Applicable major release
Name: IK8752295 (7870) Type: equipmentAlarm Package: lmg.IK8752295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2597 IK8752302

Alarm	Attributes	Applicable major release
Name: IK8752302 (7871) Type: equipmentAlarm Package: lmg.IK8752302 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2598 IK8752337

Alarm	Attributes	Applicable major release
Name: IK8752337 (7872) Type: communicationsAlarm Package: lmg.IK8752337 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2599 IK8752341

Alarm	Attributes	Applicable major release
Name: IK8752341 (7873) Type: communicationsAlarm Package: Img.IK8752341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2600 IK8752343

Alarm	Attributes	Applicable major release
Name: IK8752343 (7874) Type: communicationsAlarm Package: Img.IK8752343 Raised on class: Img.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2601 IK8752347

Alarm	Attributes	Applicable major release
Name: IK8752347 (7875) Type: communicationsAlarm Package: Img.IK8752347 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2602 IK8752349

Alarm	Attributes	Applicable major release
Name: IK8752349 (7876) Type: communicationsAlarm Package: lmg.IK8752349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2603 IK8752360

Alarm	Attributes	Applicable major release
Name: IK8752360 (7877) Type: equipmentAlarm Package: lmg.IK8752360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-2604 IK8752363

Alarm	Attributes	Applicable major release
Name: IK8752363 (7878) Type: environmentalAlarm Package: lmg.IK8752363 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2605 IK8752368

Alarm	Attributes	Applicable major release
Name: IK8752368 (7879) Type: equipmentAlarm Package: Img.IK8752368 Raised on class: Img.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2606 IK8752369

Alarm	Attributes	Applicable major release
Name: IK8752369 (7880) Type: equipmentAlarm Package: Img.IK8752369 Raised on class: Img.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2607 IK8752374

Alarm	Attributes	Applicable major release
Name: IK8752374 (7881) Type: equipmentAlarm Package: Img.IK8752374 Raised on class: Img.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-2608 IK8752375

Alarm	Attributes	Applicable major release
Name: IK8752375 (7882) Type: equipmentAlarm Package: lmg.IK8752375 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-2609 IK8752376

Alarm	Attributes	Applicable major release
Name: IK8752376 (7883) Type: equipmentAlarm Package: lmg.IK8752376 Raised on class: lmg.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-2610 IK8752377

Alarm	Attributes	Applicable major release
Name: IK8752377 (7884) Type: equipmentAlarm Package: lmg.IK8752377 Raised on class: lmg.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-2611 IK8752378

Alarm	Attributes	Applicable major release
Name: IK8752378 (7885) Type: equipmentAlarm Package: Img.IK8752378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-2612 IK8752379

Alarm	Attributes	Applicable major release
Name: IK8752379 (7886) Type: equipmentAlarm Package: Img.IK8752379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-2613 IK8752380

Alarm	Attributes	Applicable major release
Name: IK8752380 (7887) Type: equipmentAlarm Package: Img.IK8752380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-2614 IK8752382

Alarm	Attributes	Applicable major release
Name: IK8752382 (7888) Type: environmentalAlarm Package: lmg.IK8752382 Raised on class: lmg.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-2615 IK8752386

Alarm	Attributes	Applicable major release
Name: IK8752386 (7889) Type: equipmentAlarm Package: lmg.IK8752386 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2616 IK8752387

Alarm	Attributes	Applicable major release
Name: IK8752387 (7890) Type: equipmentAlarm Package: lmg.IK8752387 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2617 IK8752388

Alarm	Attributes	Applicable major release
Name: IK8752388 (7891) Type: equipmentAlarm Package: Img.IK8752388 Raised on class: Img.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2618 IK8752391

Alarm	Attributes	Applicable major release
Name: IK8752391 (7892) Type: processingErrorAlarm Package: Img.IK8752391 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-2619 IK8752401

Alarm	Attributes	Applicable major release
Name: IK8752401 (7893) Type: communicationsAlarm Package: Img.IK8752401 Raised on class: Img.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-2620 IK8752408

Alarm	Attributes	Applicable major release
Name: IK8752408 (7894) Type: qualityOfServiceAlarm Package: lmg.IK8752408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2621 IK8752409

Alarm	Attributes	Applicable major release
Name: IK8752409 (7895) Type: processingErrorAlarm Package: lmg.IK8752409 Raised on class: lmg.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2622 IK8752411

Alarm	Attributes	Applicable major release
Name: IK8752411 (7896) Type: equipmentAlarm Package: lmg.IK8752411 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2623 IK8752428

Alarm	Attributes	Applicable major release
Name: IK8752428 (7897) Type: equipmentAlarm Package: lmg.IK8752428 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2623 IK8752428 (continued)

Alarm	Attributes	Applicable major release
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2624 IK8752429

Alarm	Attributes	Applicable major release
Name: IK8752429 (7898) Type: equipmentAlarm Package: Img.IK8752429 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2625 IK8752431

Alarm	Attributes	Applicable major release
Name: IK8752431 (7899) Type: equipmentAlarm Package: Img.IK8752431 Raised on class: Img.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2626 IK8752432

Alarm	Attributes	Applicable major release
Name: IK8752432 (7900) Type: equipmentAlarm Package: Img.IK8752432 Raised on class: Img.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2627 IK8752436

Alarm	Attributes	Applicable major release
Name: IK8752436 (7901) Type: equipmentAlarm Package: lmg.IK8752436 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2628 IK8752437

Alarm	Attributes	Applicable major release
Name: IK8752437 (7902) Type: equipmentAlarm Package: lmg.IK8752437 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2629 IK8752439

Alarm	Attributes	Applicable major release
Name: IK8752439 (7903) Type: communicationsAlarm Package: lmg.IK8752439 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2630 IK8752462

Alarm	Attributes	Applicable major release
Name: IK8752462 (10002) Type: environmentalAlarm Package: lmg.IK8752462 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR16.1.MG

Table 27-2630 IK8752462 (continued)

Alarm	Attributes	Applicable major release
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-2631 IK8752464

Alarm	Attributes	Applicable major release
Name: IK8752464 (10003) Type: equipmentAlarm Package: Img.IK8752464 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2632 IK8752468

Alarm	Attributes	Applicable major release
Name: IK8752468 (10004) Type: equipmentAlarm Package: Img.IK8752468 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2633 IK8752494

Alarm	Attributes	Applicable major release
Name: IK8752494 (10007) Type: equipmentAlarm Package: Img.IK8752494 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutpu-tOverload		
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-2634 IK8752496

Alarm	Attributes	Applicable major release
Name: IK8752496 (10008) Type: environmentalAlarm Package: lmg.IK8752496 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-2635 IK8752508

Alarm	Attributes	Applicable major release
Name: IK8752508 (10015) Type: equipmentAlarm Package: lmg.IK8752508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2636 IK8752510

Alarm	Attributes	Applicable major release
Name: IK8752510 (10016) Type: environmentalAlarm Package: lmg.IK8752510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2637 IK8752518

Alarm	Attributes	Applicable major release
Name: IK8752518 (10019) Type: equipmentAlarm Package: lmg.IK8752518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2638 IK8752531

Alarm	Attributes	Applicable major release
Name: IK8752531 (10024) Type: equipmentAlarm Package: lmg.IK8752531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-2639 IK8752533

Alarm	Attributes	Applicable major release
Name: IK8752533 (10025) Type: equipmentAlarm Package: lmg.IK8752533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInputOutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-2640 IK8752534

Alarm	Attributes	Applicable major release
Name: IK8752534 (10026) Type: environmentalAlarm Package: lmg.IK8752534 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTemperatureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-2641 IK8752536

Alarm	Attributes	Applicable major release
Name: IK8752536 (10027) Type: equipmentAlarm Package: lmg.IK8752536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassOnAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-2642 IK8752539

Alarm	Attributes	Applicable major release
Name: IK8752539 (10029) Type: equipmentAlarm Package: lmg.IK8752539 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-2643 IK8752541

Alarm	Attributes	Applicable major release
Name: IK8752541 (10030) Type: environmentalAlarm Package: lmg.IK8752541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR16.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-2644 IK8752543

Alarm	Attributes	Applicable major release
Name: IK8752543 (10031) Type: equipmentAlarm Package: lmg.IK8752543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2645 IK8752546

Alarm	Attributes	Applicable major release
Name: IK8752546 (10033) Type: equipmentAlarm Package: lmg.IK8752546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2646 IK8752548

Alarm	Attributes	Applicable major release
Name: IK8752548 (10034) Type: environmentalAlarm Package: lmg.IK8752548 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If the problem persists, contact NOKIA customer support.		

Table 27-2647 IK8752550

Alarm	Attributes	Applicable major release
Name: IK8752550 (10035) Type: environmentalAlarm Package: lmg.IK8752550 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If the problem persists, contact NOKIA customer support.		

Table 27-2648 IK8752552

Alarm	Attributes	Applicable major release
Name: IK8752552 (10036) Type: processingErrorAlarm Package: lmg.IK8752552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-2649 IK8752554

Alarm	Attributes	Applicable major release
Name: IK8752554 (10037) Type: equipmentAlarm Package: lmg.IK8752554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-2650 IK8752556

Alarm	Attributes	Applicable major release
Name: IK8752556 (10038) Type: equipmentAlarm Package: lmg.IK8752556 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-2651 IK8752559

Alarm	Attributes	Applicable major release
Name: IK8752559 (7904) Type: equipmentAlarm Package: lmg.IK8752559 Raised on class: lmg.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-2652 IK8752609

Alarm	Attributes	Applicable major release
Name: IK8752609 (7905) Type: processingErrorAlarm Package: lmg.IK8752609 Raised on class: lmg.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2653 IK8752610

Alarm	Attributes	Applicable major release
Name: IK8752610 (7906) Type: processingErrorAlarm Package: lmg.IK8752610 Raised on class: lmg.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2654 IK8752615

Alarm	Attributes	Applicable major release
Name: IK8752615 (7907) Type: equipmentAlarm Package: lmg.IK8752615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-2655 IK8752616

Alarm	Attributes	Applicable major release
Name: IK8752616 (7908) Type: environmentalAlarm Package: lmg.IK8752616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-2656 IK8752617

Alarm	Attributes	Applicable major release
Name: IK8752617 (7909) Type: environmentalAlarm Package: lmg.IK8752617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-2657 IK8752620

Alarm	Attributes	Applicable major release
Name: IK8752620 (7910) Type: equipmentAlarm Package: lmg.IK8752620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		
Remedial action: Check the server's power source.		

Table 27-2658 IK8752622

Alarm	Attributes	Applicable major release
Name: IK8752622 (7911) Type: environmentalAlarm Package: Img.IK8752622 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-2659 IK8752628

Alarm	Attributes	Applicable major release
Name: IK8752628 (7912) Type: equipmentAlarm Package: Img.IK8752628 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-2660 IK8752632

Alarm	Attributes	Applicable major release
Name: IK8752632 (7913) Type: processingErrorAlarm Package: Img.IK8752632 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2661 IK8752633

Alarm	Attributes	Applicable major release
Name: IK8752633 (7914) Type: communicationsAlarm Package: lmg.IK8752633 Raised on class: lmg.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-2662 IK8752636

Alarm	Attributes	Applicable major release
Name: IK8752636 (9394) Type: equipmentAlarm Package: lmg.IK8752636 Raised on class: lmg.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2663 IK8752648

Alarm	Attributes	Applicable major release
Name: IK8752648 (7915) Type: qualityOfServiceAlarm Package: lmg.IK8752648 Raised on class: lmg.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2664 IK8752657

Alarm	Attributes	Applicable major release
Name: IK8752657 (7916) Type: environmentalAlarm Package: lmg.IK8752657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2665 IK8754762

Alarm	Attributes	Applicable major release
Name: IK8754762 (7917) Type: communicationsAlarm Package: lmg.IK8754762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2666 IK8757481

Alarm	Attributes	Applicable major release
Name: IK8757481 (10886) Type: equipmentAlarm Package: lmg.IK8757481 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.		
Remedial action: No action is required.		

Table 27-2667 IK8757482

Alarm	Attributes	Applicable major release
Name: IK8757482 (10887) Type: equipmentAlarm Package: Img.IK8757482 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.		
Remedial action: No action is required.		

Table 27-2668 IK8757483

Alarm	Attributes	Applicable major release
Name: IK8757483 (10888) Type: equipmentAlarm Package: Img.IK8757483 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.		
Remedial action: No action is required.		

Table 27-2669 IK8757484

Alarm	Attributes	Applicable major release
Name: IK8757484 (10889) Type: equipmentAlarm Package: Img.IK8757484 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.		
Remedial action: No action is required.		

Table 27-2670 IK8757485

Alarm	Attributes	Applicable major release
Name: IK8757485 (10890) Type: equipmentAlarm Package: Img.IK8757485 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR16.1.MG
Description: A disk drive has failed. Details: A disk device has failed.		
Remedial action: No action is required.		

Table 27-2671 IK8757486

Alarm	Attributes	Applicable major release
Name: IK8757486 (10891) Type: equipmentAlarm Package: lmg.IK8757486 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-2672 IK8757487

Alarm	Attributes	Applicable major release
Name: IK8757487 (10892) Type: equipmentAlarm Package: lmg.IK8757487 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.		
Remedial action: No action is required.		

Table 27-2673 IK8757488

Alarm	Attributes	Applicable major release
Name: IK8757488 (10893) Type: equipmentAlarm Package: lmg.IK8757488 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-2674 IK8757489

Alarm	Attributes	Applicable major release
Name: IK8757489 (10894) Type: equipmentAlarm Package: lmg.IK8757489 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.		

Table 27-2674 IK8757489 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2675 IK8757490

Alarm	Attributes	Applicable major release
Name: IK8757490 (10895) Type: equipmentAlarm Package: Img.IK8757490 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.		
Remedial action: No action is required.		

Table 27-2676 IK8757491

Alarm	Attributes	Applicable major release
Name: IK8757491 (10896) Type: equipmentAlarm Package: Img.IK8757491 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.		
Remedial action: No action is required.		

Table 27-2677 IK8757500

Alarm	Attributes	Applicable major release
Name: IK8757500 (10897) Type: equipmentAlarm Package: Img.IK8757500 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes degraded.		
Remedial action: No action is required.		

Table 27-2678 IK8757501

Alarm	Attributes	Applicable major release
Name: IK8757501 (10898) Type: equipmentAlarm Package: lmg.IK8757501 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a node in the cluster becomes failed.		
Remedial action: No action is required.		

Table 27-2679 IK8757502

Alarm	Attributes	Applicable major release
Name: IK8757502 (10899) Type: equipmentAlarm Package: lmg.IK8757502 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes degraded.		
Remedial action: No action is required.		

Table 27-2680 IK8757503

Alarm	Attributes	Applicable major release
Name: IK8757503 (10900) Type: equipmentAlarm Package: lmg.IK8757503 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster resource becomes failed.		
Remedial action: No action is required.		

Table 27-2681 IK8757504

Alarm	Attributes	Applicable major release
Name: IK8757504 (10901) Type: equipmentAlarm Package: lmg.IK8757504 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes degraded.		

Table 27-2681 IK8757504 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2682 IK8757505

Alarm	Attributes	Applicable major release
Name: IK8757505 (10902) Type: equipmentAlarm Package: lmg.IK8757505 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: This event will be sent any time the condition of a cluster network becomes failed.		
Remedial action: No action is required.		

Table 27-2683 IK8757508

Alarm	Attributes	Applicable major release
Name: IK8757508 (10903) Type: equipmentAlarm Package: lmg.IK8757508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2684 IK8757509

Alarm	Attributes	Applicable major release
Name: IK8757509 (10904) Type: equipmentAlarm Package: lmg.IK8757509 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-2685 IK8757510

Alarm	Attributes	Applicable major release
Name: IK8757510 (10905) Type: equipmentAlarm Package: lmg.IK8757510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: External Array Redundant Controller Active. This event signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.		
Remedial action: No action is required.		

Table 27-2686 IK8757511

Alarm	Attributes	Applicable major release
Name: IK8757511 (10906) Type: equipmentAlarm Package: lmg.IK8757511 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: External Array Accelerator Board Bad Data. This event signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2687 IK8757512

Alarm	Attributes	Applicable major release
Name: IK8757512 (10907) Type: equipmentAlarm Package: lmg.IK8757512 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: External Array Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.		
Remedial action: No action is required.		

Table 27-2688 IK8757513

Alarm	Attributes	Applicable major release
Name: IK8757513 (10908) Type: equipmentAlarm Package: Img.IK8757513 Raised on class: Img.FRU	Severity: indeterminate Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log		
Remedial action: No action is required.		

Table 27-2689 IK8757514

Alarm	Attributes	Applicable major release
Name: IK8757514 (10909) Type: equipmentAlarm Package: Img.IK8757514 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.		
Remedial action: No action is required.		

Table 27-2690 IK8757515

Alarm	Attributes	Applicable major release
Name: IK8757515 (10910) Type: equipmentAlarm Package: Img.IK8757515 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-2691 IK8757516

Alarm	Attributes	Applicable major release
Name: IK8757516 (10911) Type: equipmentAlarm Package: Img.IK8757516 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.		
Remedial action: No action is required.		

Table 27-2692 IK8757517

Alarm	Attributes	Applicable major release
Name: IK8757517 (10912) Type: equipmentAlarm Package: lmg.IK8757517 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-2693 IK8757518

Alarm	Attributes	Applicable major release
Name: IK8757518 (10913) Type: equipmentAlarm Package: lmg.IK8757518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.		
Remedial action: No action is required.		

Table 27-2694 IK8757519

Alarm	Attributes	Applicable major release
Name: IK8757519 (10914) Type: equipmentAlarm Package: lmg.IK8757519 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.		
Remedial action: No action is required.		

Table 27-2695 IK8757520

Alarm	Attributes	Applicable major release
Name: IK8757520 (10915) Type: equipmentAlarm Package: lmg.IK8757520 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.		

Table 27-2695 IK8757520 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2696 IK8757521

Alarm	Attributes	Applicable major release
Name: IK8757521 (10916) Type: equipmentAlarm Package: lmg.IK8757521 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.		
Remedial action: No action is required.		

Table 27-2697 IK8757522

Alarm	Attributes	Applicable major release
Name: IK8757522 (10917) Type: equipmentAlarm Package: lmg.IK8757522 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.		
Remedial action: No action is required.		

Table 27-2698 IK8757523

Alarm	Attributes	Applicable major release
Name: IK8757523 (10918) Type: equipmentAlarm Package: lmg.IK8757523 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.		
Remedial action: No action is required.		

Table 27-2699 IK8757524

Alarm	Attributes	Applicable major release
Name: IK8757524 (10919) Type: equipmentAlarm Package: lmg.IK8757524 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.		
Remedial action: No action is required.		

Table 27-2700 IK8757525

Alarm	Attributes	Applicable major release
Name: IK8757525 (10920) Type: equipmentAlarm Package: lmg.IK8757525 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.		
Remedial action: No action is required.		

Table 27-2701 IK8757526

Alarm	Attributes	Applicable major release
Name: IK8757526 (10921) Type: equipmentAlarm Package: lmg.IK8757526 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.		
Remedial action: No action is required.		

Table 27-2702 IK8757527

Alarm	Attributes	Applicable major release
Name: IK8757527 (10922) Type: equipmentAlarm Package: Img.IK8757527 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.		
Remedial action: No action is required.		

Table 27-2703 IK8757528

Alarm	Attributes	Applicable major release
Name: IK8757528 (10923) Type: equipmentAlarm Package: Img.IK8757528 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-2704 IK8757529

Alarm	Attributes	Applicable major release
Name: IK8757529 (10924) Type: equipmentAlarm Package: Img.IK8757529 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.		
Remedial action: No action is required.		

Table 27-2705 IK8757530

Alarm	Attributes	Applicable major release
Name: IK8757530 (10925) Type: equipmentAlarm Package: lmg.IK8757530 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.		
Remedial action: No action is required.		

Table 27-2706 IK8757531

Alarm	Attributes	Applicable major release
Name: IK8757531 (10926) Type: equipmentAlarm Package: lmg.IK8757531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the configured redundant NIC becomes the active NIC.		
Remedial action: No action is required.		

Table 27-2707 IK8757532

Alarm	Attributes	Applicable major release
Name: IK8757532 (10927) Type: equipmentAlarm Package: lmg.IK8757532 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.MG
Description: This event is a send to the user to notify him of a Critical Software Update.		
Remedial action: No action is required.		

Table 27-2708 IK8757533

Alarm	Attributes	Applicable major release
Name: IK8757533 (10928) Type: equipmentAlarm Package: lmg.IK8757533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG

Table 27-2708 IK8757533 (continued)

Alarm	Attributes	Applicable major release
Description: Controller Active. This event signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.		
Remedial action: No action is required.		

Table 27-2709 IK8757534

Alarm	Attributes	Applicable major release
Name: IK8757534 (10929) Type: equipmentAlarm Package: lmg.IK8757534 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2710 IK8757535

Alarm	Attributes	Applicable major release
Name: IK8757535 (10930) Type: equipmentAlarm Package: lmg.IK8757535 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Accelerator Board Bad Data. This event signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.		
Remedial action: No action is required.		

Table 27-2711 IK8757536

Alarm	Attributes	Applicable major release
Name: IK8757536 (10931) Type: equipmentAlarm Package: lmg.IK8757536 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Accelerator Board Battery Failed. This event signifies that the agent has detected a battery failure associated with the array accelerator cache board.		
Remedial action: No action is required.		

Table 27-2712 IK8757537

Alarm	Attributes	Applicable major release
Name: IK8757537 (10932) Type: equipmentAlarm Package: lmg.IK8757537 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2713 IK8757538

Alarm	Attributes	Applicable major release
Name: IK8757538 (10933) Type: equipmentAlarm Package: lmg.IK8757538 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Physical Drive Threshold Passed. This event signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.		
Remedial action: No action is required.		

Table 27-2714 IK8757539

Alarm	Attributes	Applicable major release
Name: IK8757539 (10934) Type: equipmentAlarm Package: lmg.IK8757539 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Cache Module Board Bad Data. This event signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-2715 IK8757540

Alarm	Attributes	Applicable major release
Name: IK8757540 (10935) Type: equipmentAlarm Package: lmg.IK8757540 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG

Table 27-2715 IK8757540 (continued)

Alarm	Attributes	Applicable major release
Description: Cache Module Board Backup Power Source Failed. This event signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.		
Remedial action: No action is required.		

Table 27-2716 IK8757541

Alarm	Attributes	Applicable major release
Name: IK8757541 (10936) Type: equipmentAlarm Package: lmg.IK8757541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-2717 IK8757542

Alarm	Attributes	Applicable major release
Name: IK8757542 (10937) Type: equipmentAlarm Package: lmg.IK8757542 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-2718 IK8757543

Alarm	Attributes	Applicable major release
Name: IK8757543 (10938) Type: equipmentAlarm Package: lmg.IK8757543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.		
Remedial action: No action is required.		

Table 27-2719 IK8757545

Alarm	Attributes	Applicable major release
Name: IK8757545 (10939) Type: equipmentAlarm Package: lmg.IK8757545 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: This event will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.		
Remedial action: No action is required.		

Table 27-2720 IK8757546

Alarm	Attributes	Applicable major release
Name: IK8757546 (10940) Type: equipmentAlarm Package: lmg.IK8757546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to failed. This event signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-2721 IK8757547

Alarm	Attributes	Applicable major release
Name: IK8757547 (10941) Type: equipmentAlarm Package: lmg.IK8757547 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR16.1.MG
Description: The enclosure fan status has been set to degraded. This event signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.		
Remedial action: No action is required.		

Table 27-2722 IK8757548

Alarm	Attributes	Applicable major release
Name: IK8757548 (10942) Type: equipmentAlarm Package: Img.IK8757548 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to failed. This event signifies that a power supply has failed.		
Remedial action: No action is required.		

Table 27-2723 IK8757549

Alarm	Attributes	Applicable major release
Name: IK8757549 (10943) Type: equipmentAlarm Package: Img.IK8757549 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The power supply status has been set to degraded. This event signifies that a power supply has degraded.		
Remedial action: No action is required.		

Table 27-2724 IK8757550

Alarm	Attributes	Applicable major release
Name: IK8757550 (10944) Type: equipmentAlarm Package: Img.IK8757550 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem is no longer in a redundant state.		
Remedial action: No action is required.		

Table 27-2725 IK8757551

Alarm	Attributes	Applicable major release
Name: IK8757551 (10945) Type: equipmentAlarm Package: Img.IK8757551 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power supply detected an input line voltage problem.		

Table 27-2725 IK8757551 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2726 IK8757552

Alarm	Attributes	Applicable major release
Name: IK8757552 (10946) Type: equipmentAlarm Package: lmg.IK8757552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: The rack power subsystem overload condition.		
Remedial action: No action is required.		

Table 27-2727 IK8757553

Alarm	Attributes	Applicable major release
Name: IK8757553 (10947) Type: equipmentAlarm Package: lmg.IK8757553 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.		
Remedial action: No action is required.		

Table 27-2728 IK8757554

Alarm	Attributes	Applicable major release
Name: IK8757554 (10948) Type: equipmentAlarm Package: lmg.IK8757554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.		
Remedial action: No action is required.		

Table 27-2729 IK8757555

Alarm	Attributes	Applicable major release
Name: IK8757555 (10949) Type: equipmentAlarm Package: Img.IK8757555 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.		
Remedial action: No action is required.		

Table 27-2730 IK8757556

Alarm	Attributes	Applicable major release
Name: IK8757556 (10950) Type: equipmentAlarm Package: Img.IK8757556 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-2731 IK8757557

Alarm	Attributes	Applicable major release
Name: IK8757557 (10951) Type: equipmentAlarm Package: Img.IK8757557 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.		
Remedial action: No action is required.		

Table 27-2732 IK8757558

Alarm	Attributes	Applicable major release
Name: IK8757558 (10952) Type: equipmentAlarm Package: Img.IK8757558 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Fuse open. The fuse has been tripped.		

Table 27-2732 IK8757558 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2733 IK8757559

Alarm	Attributes	Applicable major release
Name: IK8757559 (10953) Type: equipmentAlarm Package: lmg.IK8757559 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.		
Remedial action: No action is required.		

Table 27-2734 IK8757560

Alarm	Attributes	Applicable major release
Name: IK8757560 (10954) Type: equipmentAlarm Package: lmg.IK8757560 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.		
Remedial action: No action is required.		

Table 27-2735 IK8757561

Alarm	Attributes	Applicable major release
Name: IK8757561 (10955) Type: equipmentAlarm Package: lmg.IK8757561 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.		
Remedial action: No action is required.		

Table 27-2736 IK8757562

Alarm	Attributes	Applicable major release
Name: IK8757562 (10956) Type: equipmentAlarm Package: Img.IK8757562 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.		
Remedial action: No action is required.		

Table 27-2737 IK8757563

Alarm	Attributes	Applicable major release
Name: IK8757563 (10957) Type: equipmentAlarm Package: Img.IK8757563 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.		
Remedial action: No action is required.		

Table 27-2738 IK8757564

Alarm	Attributes	Applicable major release
Name: IK8757564 (10958) Type: equipmentAlarm Package: Img.IK8757564 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.		
Remedial action: No action is required.		

Table 27-2739 IK8757565

Alarm	Attributes	Applicable major release
Name: IK8757565 (10959) Type: equipmentAlarm Package: Img.IK8757565 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG

Table 27-2739 IK8757565 (continued)

Alarm	Attributes	Applicable major release
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.		
Remedial action: No action is required.		

Table 27-2740 IK8757566

Alarm	Attributes	Applicable major release
Name: IK8757566 (10960) Type: equipmentAlarm Package: Img.IK8757566 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.		
Remedial action: No action is required.		

Table 27-2741 IK8757567

Alarm	Attributes	Applicable major release
Name: IK8757567 (10961) Type: equipmentAlarm Package: Img.IK8757567 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper		
Remedial action: No action is required.		

Table 27-2742 IK8757568

Alarm	Attributes	Applicable major release
Name: IK8757568 (10962) Type: equipmentAlarm Package: Img.IK8757568 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.		
Remedial action: No action is required.		

Table 27-2743 IK8757569

Alarm	Attributes	Applicable major release
Name: IK8757569 (10963) Type: equipmentAlarm Package: Img.IK8757569 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.		
Remedial action: No action is required.		

Table 27-2744 IK8757570

Alarm	Attributes	Applicable major release
Name: IK8757570 (10964) Type: equipmentAlarm Package: Img.IK8757570 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.		
Remedial action: No action is required.		

Table 27-2745 IK8757571

Alarm	Attributes	Applicable major release
Name: IK8757571 (10965) Type: equipmentAlarm Package: Img.IK8757571 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.		
Remedial action: No action is required.		

Table 27-2746 IK8757572

Alarm	Attributes	Applicable major release
Name: IK8757572 (10966) Type: equipmentAlarm Package: Img.IK8757572 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Generic WSMAN Major trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-2746 IK8757572 (continued)

Alarm	Attributes	Applicable major release
Description: WSMAN Major trap		
Remedial action: No action is required.		

Table 27-2747 IK8757573

Alarm	Attributes	Applicable major release
Name: IK8757573 (10967) Type: equipmentAlarm Package: lmg.IK8757573 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Generic WSMAN Critical trap Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: WSMAN Critical trap		
Remedial action: No action is required.		

Table 27-2748 IK8757574

Alarm	Attributes	Applicable major release
Name: IK8757574 (10968) Type: equipmentAlarm Package: lmg.IK8757574 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-2749 IK8757575

Alarm	Attributes	Applicable major release
Name: IK8757575 (10969) Type: equipmentAlarm Package: lmg.IK8757575 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR16.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.		
Remedial action: No action is required.		

Table 27-2750 IK8757576

Alarm	Attributes	Applicable major release
Name: IK8757576 (10970) Type: equipmentAlarm Package: Img.IK8757576 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting input voltage is out of range.		
Remedial action: No action is required.		

Table 27-2751 IK8757577

Alarm	Attributes	Applicable major release
Name: IK8757577 (10971) Type: equipmentAlarm Package: Img.IK8757577 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-2752 IK8757578

Alarm	Attributes	Applicable major release
Name: IK8757578 (10972) Type: equipmentAlarm Package: Img.IK8757578 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting low battery.		
Remedial action: No action is required.		

Table 27-2753 IK8757579

Alarm	Attributes	Applicable major release
Name: IK8757579 (10973) Type: equipmentAlarm Package: Img.IK8757579 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-2754 IK8757580

Alarm	Attributes	Applicable major release
Name: IK8757580 (10974) Type: equipmentAlarm Package: Img.IK8757580 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.		
Remedial action: No action is required.		

Table 27-2755 IK8757581

Alarm	Attributes	Applicable major release
Name: IK8757581 (10975) Type: equipmentAlarm Package: Img.IK8757581 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.		
Remedial action: No action is required.		

Table 27-2756 IK8757582

Alarm	Attributes	Applicable major release
Name: IK8757582 (10976) Type: equipmentAlarm Package: Img.IK8757582 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting on battery condition.		
Remedial action: No action is required.		

Table 27-2757 IK8757583

Alarm	Attributes	Applicable major release
Name: IK8757583 (10977) Type: equipmentAlarm Package: Img.IK8757583 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: A UPS device is reporting temperature is out of range.		

Table 27-2757 IK8757583 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2758 IK8757584

Alarm	Attributes	Applicable major release
Name: IK8757584 (10978) Type: equipmentAlarm Package: Img.IK8757584 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-2759 IK8757585

Alarm	Attributes	Applicable major release
Name: IK8757585 (10979) Type: equipmentAlarm Package: Img.IK8757585 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting a diagnostic test failed.		
Remedial action: No action is required.		

Table 27-2760 IK8757586

Alarm	Attributes	Applicable major release
Name: IK8757586 (10980) Type: equipmentAlarm Package: Img.IK8757586 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-2761 IK8757587

Alarm	Attributes	Applicable major release
Name: IK8757587 (10981) Type: equipmentAlarm Package: lmg.IK8757587 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.		
Remedial action: No action is required.		

Table 27-2762 IK8757588

Alarm	Attributes	Applicable major release
Name: IK8757588 (10982) Type: equipmentAlarm Package: lmg.IK8757588 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-2763 IK8757589

Alarm	Attributes	Applicable major release
Name: IK8757589 (10983) Type: equipmentAlarm Package: lmg.IK8757589 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is operating in manual bypass mode.		
Remedial action: No action is required.		

Table 27-2764 IK8757590

Alarm	Attributes	Applicable major release
Name: IK8757590 (10984) Type: equipmentAlarm Package: lmg.IK8757590 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting output voltage is out of Range.		
Remedial action: No action is required.		

Table 27-2765 IK8757591

Alarm	Attributes	Applicable major release
Name: IK8757591 (10985) Type: equipmentAlarm Package: Img.IK8757591 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.		
Remedial action: No action is required.		

Table 27-2766 IK8757592

Alarm	Attributes	Applicable major release
Name: IK8757592 (10986) Type: equipmentAlarm Package: Img.IK8757592 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: A warning alarm has occurred.		
Remedial action: No action is required.		

Table 27-2767 IK8757593

Alarm	Attributes	Applicable major release
Name: IK8757593 (10987) Type: equipmentAlarm Package: Img.IK8757593 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.		
Remedial action: No action is required.		

Table 27-2768 IK8757594

Alarm	Attributes	Applicable major release
Name: IK8757594 (10988) Type: equipmentAlarm Package: Img.IK8757594 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG

Table 27-2768 IK8757594 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.		
Remedial action: No action is required.		

Table 27-2769 IK8757595

Alarm	Attributes	Applicable major release
Name: IK8757595 (10989) Type: equipmentAlarm Package: lmg.IK8757595 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR16.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.		
Remedial action: No action is required.		

Table 27-2770 IK8757596

Alarm	Attributes	Applicable major release
Name: IK8757596 (10990) Type: equipmentAlarm Package: lmg.IK8757596 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.		
Remedial action: No action is required.		

Table 27-2771 IK8757597

Alarm	Attributes	Applicable major release
Name: IK8757597 (10991) Type: equipmentAlarm Package: lmg.IK8757597 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.		
Remedial action: No action is required.		

Table 27-2772 IK8757598

Alarm	Attributes	Applicable major release
Name: IK8757598 (10992) Type: equipmentAlarm Package: Img.IK8757598 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR16.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.		
Remedial action: No action is required.		

Table 27-2773 IK8757599

Alarm	Attributes	Applicable major release
Name: IK8757599 (10993) Type: equipmentAlarm Package: Img.IK8757599 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.		
Remedial action: No action is required.		

Table 27-2774 IK8757600

Alarm	Attributes	Applicable major release
Name: IK8757600 (10994) Type: equipmentAlarm Package: Img.IK8757600 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.		
Remedial action: No action is required.		

Table 27-2775 IK8757601

Alarm	Attributes	Applicable major release
Name: IK8757601 (10995) Type: equipmentAlarm Package: Img.IK8757601 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR16.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.		

Table 27-2775 IK8757601 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 27-2776 IK8757602

Alarm	Attributes	Applicable major release
Name: IK8757602 (10996) Type: equipmentAlarm Package: Img.IK8757602 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR16.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.		
Remedial action: No action is required.		

Table 27-2777 IK8757603

Alarm	Attributes	Applicable major release
Name: IK8757603 (10997) Type: equipmentAlarm Package: Img.IK8757603 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.		
Remedial action: No action is required.		

Table 27-2778 IK8757604

Alarm	Attributes	Applicable major release
Name: IK8757604 (10998) Type: equipmentAlarm Package: Img.IK8757604 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.		
Remedial action: No action is required.		

Table 27-2779 IK8757605

Alarm	Attributes	Applicable major release
Name: IK8757605 (10999) Type: equipmentAlarm Package: lmg.IK8757605 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR16.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.		
Remedial action: No action is required.		

Table 27-2780 IK8757606

Alarm	Attributes	Applicable major release
Name: IK8757606 (11000) Type: equipmentAlarm Package: lmg.IK8757606 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.		
Remedial action: No action is required.		

Table 27-2781 IK8757607

Alarm	Attributes	Applicable major release
Name: IK8757607 (11001) Type: equipmentAlarm Package: lmg.IK8757607 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR16.1.MG
Description: A storage system power supply status has been set to degraded.		
Remedial action: No action is required.		

Table 27-2782 IK8802753

Alarm	Attributes	Applicable major release
Name: IK8802753 (7918) Type: environmentalAlarm Package: lmg.IK8802753 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: CPU temperature is too high Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG

Table 27-2782 IK8802753 (continued)

Alarm	Attributes	Applicable major release
Description: CPU temperature is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipCpuTempHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2783 IK8802755

Alarm	Attributes	Applicable major release
Name: IK8802755 (7919) Type: environmentalAlarm Package: lmg.IK8802755 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: CPU fan speed signal not received Implicitly cleared: false Default probable cause: coolingFanFailure	Release: • LR14.3.MG
Description: CPU fan speed signal not received.\nAlarm to be cleared by the operator at the management system.\nReason: bigipCpuFanSpeedBad		
Remedial action: check the CPU fan		

Table 27-2784 IK8802756

Alarm	Attributes	Applicable major release
Name: IK8802756 (7920) Type: environmentalAlarm Package: lmg.IK8802756 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Chassis temperature is too high Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: Chassis temperature is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipChassisTempHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2785 IK8802758

Alarm	Attributes	Applicable major release
Name: IK8802758 (7921) Type: equipmentAlarm Package: lmg.IK8802758 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Chassis power supply status is bad Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Chassis power supply status is bad.\nAlarm to be cleared by the operator at the management system.\nReason: bigipChassisPowerSupplyBad		
Remedial action: check the Chassis power supply		

Table 27-2786 IK8802759

Alarm	Attributes	Applicable major release
Name: IK8802759 (7922) Type: equipmentAlarm Package: Img.IK8802759 Raised on class: Img.FRU	Severity: major Specific problem: A service is detected DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A service is detected DOWN.\nAlarm is cleared by the system.\nReason: bigipServiceDown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2787 IK8802761

Alarm	Attributes	Applicable major release
Name: IK8802761 (7923) Type: equipmentAlarm Package: Img.IK8802761 Raised on class: Img.FRU	Severity: major Specific problem: A node is detected DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A node is detected DOWN.\nAlarm is cleared by the system.\nReason: bigipNodeDown		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2788 IK8802766

Alarm	Attributes	Applicable major release
Name: IK8802766 (9395) Type: equipmentAlarm Package: Img.IK8802766 Raised on class: Img.FRU	Severity: major Specific problem: A high availability feature triggered action failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A high availability feature triggered action failed.\nAlarm is cleared by the system.\nReason: bigipFeatureFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2789 IK8802778

Alarm	Attributes	Applicable major release
Name: IK8802778 (7924) Type: equipmentAlarm Package: Img.IK8802778 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: The system is in an unusable situation Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2789 IK8802778 (continued)

Alarm	Attributes	Applicable major release
Description: The system is in an unusable situation.\nAlarm to be cleared by the operator at the management system.\nReason: bigipLogEmerg		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2790 IK8802779

Alarm	Attributes	Applicable major release
Name: IK8802779 (7925) Type: equipmentAlarm Package: lmg.IK8802779 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: bigipLogAlert Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Action must be taken immediately for the system to work properly.\nAlarm to be cleared by the operator at the management system.\nReason: bigipLogAlert		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2791 IK8802780

Alarm	Attributes	Applicable major release
Name: IK8802780 (7926) Type: equipmentAlarm Package: lmg.IK8802780 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The system is in a critical condition Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The system is in a critical condition.\nAlarm to be cleared by the operator at the management system.\nReason: bigipLogCrit		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2792 IK8802787

Alarm	Attributes	Applicable major release
Name: IK8802787 (7927) Type: processingErrorAlarm Package: lmg.IK8802787 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: bigipAsmRequestBlocked Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The HTTP request was blocked because it issued (at least one) violation(s) which is marked as blocking at the current active policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmRequestBlocked		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2793 IK8802788

Alarm	Attributes	Applicable major release
Name: IK8802788 (7928) Type: processingErrorAlarm Package: lmg.IK8802788 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: bigipAsmRequestViolation Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The HTTP request issued a violation to the current active policy. This violation is marked as an alerting violation in that policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmRequestViolation		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2794 IK8802790

Alarm	Attributes	Applicable major release
Name: IK8802790 (9396) Type: equipmentAlarm Package: lmg.IK8802790 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmPoolNotAvail Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A pool is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmPoolNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2795 IK8802791

Alarm	Attributes	Applicable major release
Name: IK8802791 (9397) Type: equipmentAlarm Package: lmg.IK8802791 Raised on class: lmg.FRU	Severity: major Specific problem: A pool is disabled in global traffic management module Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A pool is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmPoolDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2796 IK8802794

Alarm	Attributes	Applicable major release
Name: IK8802794 (9398) Type: communicationsAlarm Package: lmg.IK8802794 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmLinkNotAvail Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A link is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmLinkNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2797 IK8802795

Alarm	Attributes	Applicable major release
Name: IK8802795 (9399) Type: communicationsAlarm Package: lmg.IK8802795 Raised on class: lmg.FRU	Severity: major Specific problem: A link is disabled in global traffic management module Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG • LR16.1.MG
Description: A link is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmLinkDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2798 IK8802798

Alarm	Attributes	Applicable major release
Name: IK8802798 (9400) Type: equipmentAlarm Package: lmg.IK8802798 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmWideIpNotAvail Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A wide IP is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmWideIpNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2799 IK8802799

Alarm	Attributes	Applicable major release
Name: IK8802799 (9401) Type: equipmentAlarm Package: lmg.IK8802799 Raised on class: lmg.FRU	Severity: major Specific problem: A wide IP is disabled in global traffic management module Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A wide IP is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmWideIp-Disabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2800 IK8802802

Alarm	Attributes	Applicable major release
Name: IK8802802 (9402) Type: equipmentAlarm Package: lmg.IK8802802 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmPoolMbrNotAvail Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A pool member is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmPoolMbrNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2801 IK8802803

Alarm	Attributes	Applicable major release
Name: IK8802803 (9403) Type: equipmentAlarm Package: lmg.IK8802803 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmPoolMbrDisabled Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A pool member is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmPoolMbrDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2802 IK8802806

Alarm	Attributes	Applicable major release
Name: IK8802806 (7929) Type: equipmentAlarm Package: lmg.IK8802806 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmServerNotAvail Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A server is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmServerNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2803 IK8802807

Alarm	Attributes	Applicable major release
Name: IK8802807 (9404) Type: equipmentAlarm Package: lmg.IK8802807 Raised on class: lmg.FRU	Severity: major Specific problem: A server is disabled in global traffic management module Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A server is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmServerDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2804 IK8802810

Alarm	Attributes	Applicable major release
Name: IK8802810 (9405) Type: equipmentAlarm Package: lmg.IK8802810 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmVsNotAvail Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A virtual server is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmVsNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2805 IK8802811

Alarm	Attributes	Applicable major release
Name: IK8802811 (9406) Type: equipmentAlarm Package: Img.IK8802811 Raised on class: Img.FRU	Severity: major Specific problem: bigipGtmVsDisabled Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A virtual server is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmVsDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2806 IK8802814

Alarm	Attributes	Applicable major release
Name: IK8802814 (9407) Type: processingErrorAlarm Package: Img.IK8802814 Raised on class: Img.FRU	Severity: major Specific problem: bigipGtmDcNotAvail Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: A data center is becoming unavailable in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmDcNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2807 IK8802815

Alarm	Attributes	Applicable major release
Name: IK8802815 (9408) Type: processingErrorAlarm Package: Img.IK8802815 Raised on class: Img.FRU	Severity: major Specific problem: bigipGtmDcDisabled Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: A data center is disabled in global traffic management module.\nAlarm is cleared by the system.\nReason: bigipGtmDcDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2808 IK8802819

Alarm	Attributes	Applicable major release
Name: IK8802819 (9409) Type: processingErrorAlarm Package: Img.IK8802819 Raised on class: Img.FRU	Severity: major Specific problem: bigipGtmAppObjNotAvail Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG

Table 27-2808 IK8802819 (continued)

Alarm	Attributes	Applicable major release
Description: An application object is becoming unavailable in global management module.\nAlarm is cleared by the system.\nReason: bigipGtmAppObjNotAvail		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2809 IK8802821

Alarm	Attributes	Applicable major release
Name: IK8802821 (9410) Type: processingErrorAlarm Package: lmg.IK8802821 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmAppNotAvail Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: An application is becoming unavailable in global management module.\nAlarm is cleared by the system.\nReason: bigipGtmAppNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2810 IK8802827

Alarm	Attributes	Applicable major release
Name: IK8802827 (7930) Type: communicationsAlarm Package: lmg.IK8802827 Raised on class: lmg.FRU	Severity: major Specific problem: bigipGtmBoxNotAvail Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A gtm machine (which equates to an iquery connect to a gtm machine) has gone DOWN\nAlarm is cleared by the system.\nReason: bigipGtmBoxNotAvail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2811 IK8802828

Alarm	Attributes	Applicable major release
Name: IK8802828 (7931) Type: processingErrorAlarm Package: lmg.IK8802828 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: bigipAsmFtpRequestBlocked Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The FTP request was blocked because it issued (at least one) violation(s) which is marked as blocking at the current active policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmFtpRequestBlocked		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2812 IK8802829

Alarm	Attributes	Applicable major release
Name: IK8802829 (7932) Type: processingErrorAlarm Package: Img.IK8802829 Raised on class: Img.LMGMngElement	Severity: major Specific problem: bigipAsmFtpRequestViolation Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The FTP request issued a violation to the current active policy. This violation is marked as an alerting violation in that policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmFtpRequest-Violation		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2813 IK8802834

Alarm	Attributes	Applicable major release
Name: IK8802834 (7933) Type: processingErrorAlarm Package: Img.IK8802834 Raised on class: Img.LMGMngElement	Severity: major Specific problem: bigipAsmSmtpRequestBlocked Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The SMTP request was blocked because it issued (at least one) violation(s) which is marked as blocking at the current active policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmSmtpRequestBlocked		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2814 IK8802835

Alarm	Attributes	Applicable major release
Name: IK8802835 (7934) Type: processingErrorAlarm Package: Img.IK8802835 Raised on class: Img.LMGMngElement	Severity: major Specific problem: bigipAsmSmtpRequestViolation Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: The SMTP request issued a violation to the current active policy. This violation is marked as an alerting violation in that policy in Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmSmtpRe-questViolation		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2815 IK8802836

Alarm	Attributes	Applicable major release
Name: IK8802836 (7935) Type: environmentalAlarm Package: Img.IK8802836 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Blade temperature is too high Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: Blade temperature is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipBladeTempHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2816 IK8802837

Alarm	Attributes	Applicable major release
Name: IK8802837 (7936) Type: equipmentAlarm Package: Img.IK8802837 Raised on class: Img.LMGMngElement	Severity: major Specific problem: A blade lost power Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: A blade lost power. The blade may be pulled out\nAlarm to be cleared by the operator at the management system.\nReason: bigipBladeNoPower		
Remedial action: Check the Power of the blade		

Table 27-2817 IK8802839

Alarm	Attributes	Applicable major release
Name: IK8802839 (7937) Type: equipmentAlarm Package: Img.IK8802839 Raised on class: Img.LMGMngElement	Severity: major Specific problem: offline Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: A blade has failed - offline.\nAlarm to be cleared by the operator at the management system.\nReason: bigipBladeOffline		
Remedial action: Replace the blade		

Table 27-2818 IK8802841

Alarm	Attributes	Applicable major release
Name: IK8802841 (7938) Type: processingErrorAlarm Package: Img.IK8802841 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Brute force attack detected by Application Security Module Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG

Table 27-2818 IK8802841 (continued)

Alarm	Attributes	Applicable major release
Description: Brute force attack detected by Application Security Module.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAsmBruteForceAttackDetected		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2819 IK8802842

Alarm	Attributes	Applicable major release
Name: IK8802842 (7939) Type: environmentalAlarm Package: lmg.IK8802842 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: AOM reports the air temperature near the host CPU too high Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: AOM reports the air temperature near the host CPU too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipAomCpuTempTooHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2820 IK8802845

Alarm	Attributes	Applicable major release
Name: IK8802845 (7940) Type: processingErrorAlarm Package: lmg.IK8802845 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Disk failure in a RAID disk array Implicitly cleared: false Default probable cause: storageCapacityProblem	Release: • LR14.3.MG
Description: Disk failure in a RAID disk array.\nAlarm to be cleared by the operator at the management system.\nReason: bigipRaidDiskFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2821 IK8802848

Alarm	Attributes	Applicable major release
Name: IK8802848 (9411) Type: processingErrorAlarm Package: lmg.IK8802848 Raised on class: lmg.FRU	Severity: major Specific problem: Prober Pool Disabled Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Prober Pool Disabled.\nAlarm is cleared by the system.\nReason: bigipGtmProberPoolDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2822 IK8802852

Alarm	Attributes	Applicable major release
Name: IK8802852 (9412) Type: processingErrorAlarm Package: lmg.IK8802852 Raised on class: lmg.FRU	Severity: major Specific problem: Prober Pool Member Disabled Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG • LR16.1.MG
Description: Prober Pool Member Disabled.\nAlarm is cleared by the system.\nReason: bigipGtmProberPoolMbrDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2823 IK8802857

Alarm	Attributes	Applicable major release
Name: IK8802857 (7941) Type: equipmentAlarm Package: lmg.IK8802857 Raised on class: lmg.FRU	Severity: major Specific problem: A VCMP guest is powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A VCMP guest is powered off.\nAlarm is cleared by the system.\nReason: bigipVcmpAlertsVcmpPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2824 IK8802858

Alarm	Attributes	Applicable major release
Name: IK8802858 (7942) Type: communicationsAlarm Package: lmg.IK8802858 Raised on class: lmg.FRU	Severity: major Specific problem: A VCMP guest heartbeat is lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: A VCMP guest heartbeat is lost.\nAlarm is cleared by the system.\nReason: bigipVcmpAlertsVcmpHBLost		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2825 IK8802862

Alarm	Attributes	Applicable major release
Name: IK8802862 (7943) Type: environmentalAlarm Package: lmg.IK8802862 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Temperature is too high Implicitly cleared: false Default probable cause: highTemperature	Release: • LR14.3.MG
Description: Temperature is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckA-lertTempHigh		

Table 27-2825 IK8802862 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2826 IK8802863

Alarm	Attributes	Applicable major release
Name: IK8802863 (7944) Type: equipmentAlarm Package: lmg.IK8802863 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Voltage is too high Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlert-VoltageHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2827 IK8802869

Alarm	Attributes	Applicable major release
Name: IK8802869 (7945) Type: equipmentAlarm Package: lmg.IK8802869 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Blade hardware sensor indicated critical alarm Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: Blade hardware sensor indicated critical alarm.\nAlarm to be cleared by the operator at the management system.\nReason: bigipLibhalSensorAlarmCritical		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2828 IK8802872

Alarm	Attributes	Applicable major release
Name: IK8802872 (7946) Type: equipmentAlarm Package: lmg.IK8802872 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Voltage is too low Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Voltage is too low.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlert-VoltageLow		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2829 IK8802873

Alarm	Attributes	Applicable major release
Name: IK8802873 (7947) Type: equipmentAlarm Package: Img.IK8802873 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Voltage is too high Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Milli-Voltage is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlertMilliVoltageHigh		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2830 IK8802875

Alarm	Attributes	Applicable major release
Name: IK8802875 (7948) Type: equipmentAlarm Package: Img.IK8802875 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power is too high Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Power is too high.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlertPowerHigh		
Remedial action: check the power		

Table 27-2831 IK8802876

Alarm	Attributes	Applicable major release
Name: IK8802876 (7949) Type: equipmentAlarm Package: Img.IK8802876 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Voltage is too low Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: Milli-Voltage is too low.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlertMilliVoltageLow		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2832 IK8802878

Alarm	Attributes	Applicable major release
Name: IK8802878 (7950) Type: equipmentAlarm Package: Img.IK8802878 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power is too low Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-2832 IK8802878 (continued)

Alarm	Attributes	Applicable major release
Description: Power is too low.\nAlarm to be cleared by the operator at the management system.\nReason: bigipSystemCheckAlert-PowerLow		
Remedial action: check the power		

Table 27-2833 IK8802882

Alarm	Attributes	Applicable major release
Name: IK8802882 (9413) Type: equipmentAlarm Package: lmg.IK8802882 Raised on class: lmg.FRU	Severity: major Specific problem: A DOS attack start was detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A DOS attack start was detected.\nAlarm is cleared by the system.\nReason: bigipDosAttackStart		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2834 IK8802886

Alarm	Attributes	Applicable major release
Name: IK8802886 (7951) Type: processingErrorAlarm Package: lmg.IK8802886 Raised on class: lmg.FRU	Severity: major Specific problem: Software installation has failed Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR14.3.MG • LR15.1.MG
Description: Software installation has failed.\nAlarm is cleared by the system.\nReason: emSoftwareInstallFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2835 IK8802887

Alarm	Attributes	Applicable major release
Name: IK8802887 (7952) Type: equipmentAlarm Package: lmg.IK8802887 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: A device clock is out of sync with EM Implicitly cleared: false Default probable cause: timingProblem	Release: • LR14.3.MG
Description: A device clock is out of sync with EM.\nAlarm to be cleared by the operator at the management system.\nReason: emDeviceClockSkew		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2836 IK8802889

Alarm	Attributes	Applicable major release
Name: IK8802889 (7953) Type: processingErrorAlarm Package: lmg.IK8802889 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The system memory is exceeding configured usage limits Implicitly cleared: false Default probable cause: memoryMismatch	Release: • LR14.3.MG
Description: The system memory is exceeding configured usage limits.\nAlarm to be cleared by the operator at the management system.\nReason: emMemoryUsage		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2837 IK8802891

Alarm	Attributes	Applicable major release
Name: IK8802891 (9414) Type: equipmentAlarm Package: lmg.IK8802891 Raised on class: lmg.FRU	Severity: major Specific problem: A hotfix installation has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A hotfix installation has failed.\nAlarm is cleared by the system.\nReason: emHotfixInstallFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2838 IK8802892

Alarm	Attributes	Applicable major release
Name: IK8802892 (7954) Type: equipmentAlarm Package: lmg.IK8802892 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: The cpu is exceeding configured usage limits Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: The cpu is exceeding configured usage limits.\nAlarm to be cleared by the operator at the management system.\nReason: emCpuUsage		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2839 IK8802898

Alarm	Attributes	Applicable major release
Name: IK8802898 (7955) Type: equipmentAlarm Package: Img.IK8802898 Raised on class: Img.FRU	Severity: critical Specific problem: The system RAID drive failure has been detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The system RAID drive failure has been detected.\nAlarm is cleared by the system.\nReason: emRaidDriveFailureDetected		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2840 IK8802900

Alarm	Attributes	Applicable major release
Name: IK8802900 (7956) Type: processingErrorAlarm Package: Img.IK8802900 Raised on class: Img.LMGMngElement	Severity: major Specific problem: EM HA Sync has failed Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: EM HA Sync has failed.\nAlarm to be cleared by the operator at the management system.\nReason: emHaSyncFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2841 IK8802902

Alarm	Attributes	Applicable major release
Name: IK8802902 (9415) Type: equipmentAlarm Package: Img.IK8802902 Raised on class: Img.FRU	Severity: major Specific problem: ASM signature installation has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: ASM signature installation has failed.\nAlarm is cleared by the system.\nReason: emASMSigInstallFailed		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2842 IK8802904

Alarm	Attributes	Applicable major release
Name: IK8802904 (9416) Type: equipmentAlarm Package: Img.IK8802904 Raised on class: Img.FRU	Severity: major Specific problem: ASM signature update failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: ASM signature update failed.\nAlarm is cleared by the system.\nReason: emASMSigUpdateFailed		

Table 27-2842 IK8802904 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2843 IK8802905

Alarm	Attributes	Applicable major release
Name: IK8802905 (7957) Type: processingErrorAlarm Package: lmg.IK8802905 Raised on class: lmg.FRU	Severity: major Specific problem: emPerformanceStorageDays Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: Performance storage capacity is about to fall below configured number of days.\nAlarm is cleared by the system.\ nReason: emPerformanceStorageDays		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2844 IK8802908

Alarm	Attributes	Applicable major release
Name: IK8802908 (7958) Type: processingErrorAlarm Package: lmg.IK8802908 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Scheduled performance data backup has failed Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: Scheduled performance data backup has failed.\nAlarm to be cleared by the operator at the management system.\nReason: emSchedBackupFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2845 IK8802913

Alarm	Attributes	Applicable major release
Name: IK8802913 (9417) Type: communicationsAlarm Package: lmg.IK8802913 Raised on class: lmg.FRU	Severity: major Specific problem: Statistics database connectivity is lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: Statistics database connectivity is lost.\nAlarm is cleared by the system.\nReason: emStatsDBConnectivityLost		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2846 IK8807417

Alarm	Attributes	Applicable major release
Name: IK8807417 (9418) Type: equipmentAlarm Package: Img.IK8807417 Raised on class: Img.FRU	Severity: major Specific problem: A virtual has become unavailable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A virtual has become unavailable.\nAlarm is cleared by the system.\nReason: bigipLtmVsUnavail		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2847 IK8807419

Alarm	Attributes	Applicable major release
Name: IK8807419 (9419) Type: equipmentAlarm Package: Img.IK8807419 Raised on class: Img.FRU	Severity: major Specific problem: A virtual has become disabled Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG • LR16.1.MG
Description: A virtual has become disabled.\nAlarm is cleared by the system.\nReason: bigipLtmVsDisabled		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2848 IK8807429

Alarm	Attributes	Applicable major release
Name: IK8807429 (9420) Type: equipmentAlarm Package: Img.IK8807429 Raised on class: Img.FRU	Severity: critical Specific problem: Power supply unit has powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG • LR16.1.MG
Description: Power supply unit has powered off.\nAlarm is cleared by the system.\nReason: bigipPsPowerOff		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2849 IK8850006

Alarm	Attributes	Applicable major release
Name: IK8850006 (10039) Type: processingErrorAlarm Package: Img.IK8850006 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Trap send in an alarm rising and falling edges Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR16.1.MG
Description: Trap send in an alarm rising and falling edges.\nAlarm is cleared by the system.\nReason: alarmTrap		
Remedial action: If the problem persists, contact NOKIA customer support.		

Table 27-2850 IK8900005

Alarm	Attributes	Applicable major release
Name: IK8900005 (9421) Type: processingErrorAlarm Package: lmg.IK8900005 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: mcdp alarm trap v1 Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: mcdp alarm alarm v1.\nAlarm is cleared by the system.\nReason: alarmTrapV1		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2851 IK8900006

Alarm	Attributes	Applicable major release
Name: IK8900006 (9422) Type: processingErrorAlarm Package: lmg.IK8900006 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Trap associated to an alarm of the managed element Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: Trap associated to an alarm of the managed element.\nAlarm is cleared by the system.\nReason: alarmTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2852 IK8900007

Alarm	Attributes	Applicable major release
Name: IK8900007 (9423) Type: processingErrorAlarm Package: lmg.IK8900007 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: softwareFailure Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.MG
Description: Trap associated to an alarm while executing software operation (download, activation, validation, reject, backup).\nAlarm is cleared by the system.\nReason: softwareFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2853 IK8900981

Alarm	Attributes	Applicable major release
Name: IK8900981 (9424) Type: equipmentAlarm Package: lmg.IK8900981 Raised on class: lmg.FRU	Severity: minor Specific problem: Cluster Node Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG

Table 27-2853 IK8900981 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm will be sent any time the condition of a node in the cluster becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeDegraded		
Remedial action: Make a note of the cluster node name then check the node for the cause of the degraded condition.		

Table 27-2854 IK8900982

Alarm	Attributes	Applicable major release
Name: IK8900982 (8288) Type: equipmentAlarm Package: lmg.IK8900982 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Node Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a node in the cluster becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNodeFailed		
Remedial action: Make a note of the cluster node name then check the node for the cause of the failure.		

Table 27-2855 IK8900983

Alarm	Attributes	Applicable major release
Name: IK8900983 (9425) Type: processingErrorAlarm Package: lmg.IK8900983 Raised on class: lmg.FRU	Severity: minor Specific problem: Cluster Resource Degraded Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceDegraded		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the degraded condition.		

Table 27-2856 IK8900984

Alarm	Attributes	Applicable major release
Name: IK8900984 (8289) Type: processingErrorAlarm Package: lmg.IK8900984 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Resource Failed Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster resource becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterResourceFailed		
Remedial action: Make a note of the cluster resource name then check the resource for the cause of the failure.		

Table 27-2857 IK8900985

Alarm	Attributes	Applicable major release
Name: IK8900985 (9426) Type: equipmentAlarm Package: lmg.IK8900985 Raised on class: lmg.FRU	Severity: minor Specific problem: Cluster Network Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkDegraded		
Remedial action: Make a note of the cluster network name then check the network for the cause of the degraded condition.		

Table 27-2858 IK8900986

Alarm	Attributes	Applicable major release
Name: IK8900986 (8290) Type: equipmentAlarm Package: lmg.IK8900986 Raised on class: lmg.FRU	Severity: major Specific problem: Cluster Network Failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the condition of a cluster network becomes failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqClusterNetworkFailed		
Remedial action: Make a note of the cluster network name then check the network for the cause of the failure.		

Table 27-2859 IK8901008

Alarm	Attributes	Applicable major release
Name: IK8901008 (8291) Type: equipmentAlarm Package: lmg.IK8901008 Raised on class: lmg.FRU	Severity: major Specific problem: The primary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The primary controller in the subsystem has failed. Details: The primary Controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController1FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2860 IK8901010

Alarm	Attributes	Applicable major release
Name: IK8901010 (8292) Type: equipmentAlarm Package: Img.IK8901010 Raised on class: Img.FRU	Severity: major Specific problem: The secondary controller in the subsytem has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The secondary controller in the subsystem has failed. Details: The secondary controller has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrController2FailureTrap		
Remedial action: Replace controller. Possible causes are controller physically removed, actual hardware failure.		

Table 27-2861 IK8901013

Alarm	Attributes	Applicable major release
Name: IK8901013 (8293) Type: equipmentAlarm Package: Img.IK8901013 Raised on class: Img.FRU	Severity: major Specific problem: A RAIDset has failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A RAIDset has failed. Details: The RAIDset has failed and is off-line.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveFailureTrap		
Remedial action: Possible cause is too many failed disk drives that make up the RAIDset, the OS can no longer communicate with the RAIDset for other reasons.		

Table 27-2862 IK8901015

Alarm	Attributes	Applicable major release
Name: IK8901015 (9427) Type: equipmentAlarm Package: Img.IK8901015 Raised on class: Img.FRU	Severity: minor Specific problem: A RAIDset has become degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A RAIDset has become degraded. Details: A RAIDset has become degraded due to a member disk device failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrLogDriveReducedTrap		
Remedial action: Replace the failed disk device; add a spare to the system to cause a reconstruct.		

Table 27-2863 IK8901018

Alarm	Attributes	Applicable major release
Name: IK8901018 (8294) Type: processingErrorAlarm Package: lmg.IK8901018 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system.\nReason: cpqCrDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2864 IK8901023

Alarm	Attributes	Applicable major release
Name: IK8901023 (8295) Type: processingErrorAlarm Package: lmg.IK8901023 Raised on class: lmg.FRU	Severity: major Specific problem: A disk drive has failed Implicitly cleared: true Default probable cause: storageCapacityProblem	Release: • LR14.3.MG • LR15.1.MG
Description: A disk drive has failed. Details: A disk device has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrPhyDiskFailureTrap		
Remedial action: Replace the disk device.		

Table 27-2865 IK8901028

Alarm	Attributes	Applicable major release
Name: IK8901028 (9428) Type: environmentalAlarm Package: lmg.IK8901028 Raised on class: lmg.FRU	Severity: minor Specific problem: Fan has failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: Fan has failed. Details: One of the cooling fans in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUFanFailureTrap		
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-2866 IK8901030

Alarm	Attributes	Applicable major release
Name: IK8901030 (8296) Type: equipmentAlarm Package: lmg.IK8901030 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG

Table 27-2866 IK8901030 (continued)

Alarm	Attributes	Applicable major release
Description: Power supply has failed. Details: One of the power supplies in the primary enclosure has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2867 IK8901032

Alarm	Attributes	Applicable major release
Name: IK8901032 (9429) Type: equipmentAlarm Package: lmg.IK8901032 Raised on class: lmg.FRU	Severity: warning Specific problem: Primary enclosure temperature warning Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Primary enclosure temperature warning. Details: The temperature in the primary enclosure has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrEMUTemperature-WarningTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-2868 IK8901033

Alarm	Attributes	Applicable major release
Name: IK8901033 (8297) Type: equipmentAlarm Package: lmg.IK8901033 Raised on class: lmg.FRU	Severity: critical Specific problem: Primary enclosure temperature critical! Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Primary enclosure temperature critical!. Details: The temperature in the primary enclosure has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrEMUTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the primary enclosure.		

Table 27-2869 IK8901035

Alarm	Attributes	Applicable major release
Name: IK8901035 (9430) Type: environmentalAlarm Package: lmg.IK8901035 Raised on class: lmg.FRU	Severity: minor Specific problem: Fan has failed in expansion cabinet Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: Fan has failed in expansion cabinet. Details: One of the cooling fans in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabFanFailureTrap		

Table 27-2869 IK8901035 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the cooling fan. Possible causes are fan physically removed, actual hardware failure.		

Table 27-2870 IK8901037

Alarm	Attributes	Applicable major release
Name: IK8901037 (8298) Type: equipmentAlarm Package: lmg.IK8901037 Raised on class: lmg.FRU	Severity: major Specific problem: Power supply has failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power supply has failed. Details: One of the power supplies in the expansion cabinet has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabPowerSupplyFailureTrap		
Remedial action: Replace the power supply. Possible causes are power supply physically removed, power cord unplugged, actual hardware failure.		

Table 27-2871 IK8901039

Alarm	Attributes	Applicable major release
Name: IK8901039 (9431) Type: environmentalAlarm Package: lmg.IK8901039 Raised on class: lmg.FRU	Severity: warning Specific problem: Expansion cabinet temperature warning Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: Expansion cabinet temperature warning. Details: The temperature in the expansion cabinet has triggered a warning condition detected by the controller.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCrExpCabTemperatureWarningTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-2872 IK8901040

Alarm	Attributes	Applicable major release
Name: IK8901040 (8299) Type: environmentalAlarm Package: lmg.IK8901040 Raised on class: lmg.FRU	Severity: critical Specific problem: cpqCrExpCabTemperatureCriticalTrap Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Expansion cabinet temperature critical! Details: The temperature in the expansion cabinet has triggered a critical condition detected by the controller.\nAlarm is cleared by the system.\nReason: cpqCrExpCabTemperatureCriticalTrap		
Remedial action: Check the cooling fans in the expansion cabinet.		

Table 27-2873 IK8901059

Alarm	Attributes	Applicable major release
Name: IK8901059 (9432) Type: equipmentAlarm Package: lmg.IK8901059 Raised on class: lmg.FRU	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2874 IK8901060

Alarm	Attributes	Applicable major release
Name: IK8901060 (8300) Type: environmentalAlarm Package: lmg.IK8901060 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaAccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2875 IK8901068

Alarm	Attributes	Applicable major release
Name: IK8901068 (9433) Type: processingErrorAlarm Package: lmg.IK8901068 Raised on class: lmg.FRU	Severity: warning Specific problem: External Array Redundant Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: External Array Redundant Controller Active. This alarm signifies that the Storage Agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqFcaCntlrBoxIoSlot indicates the new active controller index.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFcaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-2876 IK8901072

Alarm	Attributes	Applicable major release
Name: IK8901072 (9434) Type: equipmentAlarm Package: lmg.IK8901072 Raised on class: lmg.FRU	Severity: warning Specific problem: External Array Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: External Array Accelerator Board Bad Data. This alarm signifies that the agent has detected a Array Accelerator Cache Board that has lost battery power. If data was being stored in the accelerator memory when the system lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2877 IK8901073

Alarm	Attributes	Applicable major release
Name: IK8901073 (8301) Type: environmentalAlarm Package: lmg.IK8901073 Raised on class: lmg.FRU	Severity: major Specific problem: External Array Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: External Array Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the Array Accelerator Cache Board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqFca2AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2878 IK8901088

Alarm	Attributes	Applicable major release
Name: IK8901088 (9435) Type: environmentalAlarm Package: lmg.IK8901088 Raised on class: lmg.FRU	Severity: minor Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHeThermalTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2879 IK8901091

Alarm	Attributes	Applicable major release
Name: IK8901091 (9436) Type: environmentalAlarm Package: lmg.IK8901091 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHeThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2880 IK8901094

Alarm	Attributes	Applicable major release
Name: IK8901094 (9437) Type: environmentalAlarm Package: lmg.IK8901094 Raised on class: lmg.FRU	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHeThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2881 IK8901098

Alarm	Attributes	Applicable major release
Name: IK8901098 (8302) Type: equipmentAlarm Package: lmg.IK8901098 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHePostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2882 IK8901102

Alarm	Attributes	Applicable major release
Name: IK8901102 (8303) Type: environmentalAlarm Package: lmg.IK8901102 Raised on class: lmg.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG

Table 27-2882 IK8901102 (continued)

Alarm	Attributes	Applicable major release
Description: The temperature status has been set to failed. The system will be shutdown due to this thermal condition.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2883 IK8901103

Alarm	Attributes	Applicable major release
Name: IK8901103 (9438) Type: environmentalAlarm Package: lmg.IK8901103 Raised on class: lmg.FRU	Severity: minor Specific problem: Temperature Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature status has been set to degraded. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalTempDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2884 IK8901105

Alarm	Attributes	Applicable major release
Name: IK8901105 (8304) Type: environmentalAlarm Package: lmg.IK8901105 Raised on class: lmg.FRU	Severity: major Specific problem: System Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The system fan status has been set to failed. A required system fan is not operating normally. The system will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2885 IK8901106

Alarm	Attributes	Applicable major release
Name: IK8901106 (9439) Type: environmentalAlarm Package: lmg.IK8901106 Raised on class: lmg.FRU	Severity: minor Specific problem: System Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The system fan status has been set to degraded. An optional system fan is not operating normally.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalSystemFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2886 IK8901108

Alarm	Attributes	Applicable major release
Name: IK8901108 (9440) Type: environmentalAlarm Package: Img.IK8901108 Raised on class: Img.FRU	Severity: minor Specific problem: CPU Fan Failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The CPU fan status has been set to failed. A processor fan is not operating normally. The server will be shutdown.\nAlarm is cleared by the system.\nReason: cpqHe3ThermalCpuFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2887 IK8901112

Alarm	Attributes	Applicable major release
Name: IK8901112 (8305) Type: equipmentAlarm Package: Img.IK8901112 Raised on class: Img.FRU	Severity: major Specific problem: POST Errors Occurred Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: One or more POST errors occurred. Power On Self-Test (POST) errors occur during the server restart process. Details of the POST error messages can be found in Integrated Management Log\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PostError		
Remedial action: Refer to the Integrated Management Log for details on the POST error.		

Table 27-2888 IK8901113

Alarm	Attributes	Applicable major release
Name: IK8901113 (9441) Type: equipmentAlarm Package: Img.IK8901113 Raised on class: Img.FRU	Severity: minor Specific problem: Server Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The fault tolerant power supply sub-system condition has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolPwrSupplyDegraded		
Remedial action: Check the system for a power supply failure. Replace the power supply.		

Table 27-2889 IK8901116

Alarm	Attributes	Applicable major release
Name: IK8901116 (8306) Type: equipmentAlarm Package: Img.IK8901116 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG

Table 27-2889 IK8901116 (continued)

Alarm	Attributes	Applicable major release
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerSupplyFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2890 IK8901117

Alarm	Attributes	Applicable major release
Name: IK8901117 (9442) Type: equipmentAlarm Package: lmg.IK8901117 Raised on class: lmg.FRU	Severity: minor Specific problem: Power Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The Fault Tolerant Power Supplies have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolPowerRedundancyLost		
Remedial action: Check the system power supplies for a failure.		

Table 27-2891 IK8901120

Alarm	Attributes	Applicable major release
Name: IK8901120 (9443) Type: environmentalAlarm Package: lmg.IK8901120 Raised on class: lmg.FRU	Severity: minor Specific problem: Fan Degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to degraded for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2892 IK8901121

Alarm	Attributes	Applicable major release
Name: IK8901121 (8307) Type: environmentalAlarm Package: lmg.IK8901121 Raised on class: lmg.FRU	Severity: major Specific problem: Fan Failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The Fault Tolerant Fan condition has been set to failed for the specified chassis and fan.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3FltTolFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2893 IK8901122

Alarm	Attributes	Applicable major release
Name: IK8901122 (9444) Type: environmentalAlarm Package: Img.IK8901122 Raised on class: Img.FRU	Severity: minor Specific problem: Fan Redundancy Lost Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The Fault Tolerant Fans have lost redundancy for the specified chassis.\nAlarm is cleared by the system.\nReason: cpqHe3FltTolFanRedundancyLost		
Remedial action: Check the system fans for a failure.		

Table 27-2894 IK8901125

Alarm	Attributes	Applicable major release
Name: IK8901125 (8308) Type: environmentalAlarm Package: Img.IK8901125 Raised on class: Img.FRU	Severity: major Specific problem: Thermal Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: The temperature status has been set to failed in the specified chassis and location. The system will be shutdown due to this condition.\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureFailed		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2895 IK8901126

Alarm	Attributes	Applicable major release
Name: IK8901126 (9445) Type: environmentalAlarm Package: Img.IK8901126 Raised on class: Img.FRU	Severity: minor Specific problem: Thermal Status Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature status has been set to degraded in the specified chassis and location. The server's temperature is outside of the normal operating range. The server will be shutdown if the cpqHeThermalDegradedAction variable is set to shutdown(3).\nAlarm is cleared by the system.\nReason: cpqHe3TemperatureDegraded		
Remedial action: Check the system for hardware failures and verify the environment is properly cooled.		

Table 27-2896 IK8901128

Alarm	Attributes	Applicable major release
Name: IK8901128 (9446) Type: equipmentAlarm Package: Img.IK8901128 Raised on class: Img.FRU	Severity: minor Specific problem: Power Converter Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG

Table 27-2896 IK8901128 (continued)

Alarm	Attributes	Applicable major release
Description: The DC-DC Power Converter condition has been set to degraded for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterDegraded		
Remedial action: Check for a failing power converter or for a failed power converter in a redundant pair. Replace the power converter.		

Table 27-2897 IK8901129

Alarm	Attributes	Applicable major release
Name: IK8901129 (8309) Type: equipmentAlarm Package: lmg.IK8901129 Raised on class: lmg.FRU	Severity: major Specific problem: Power Converter Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The DC-DC Power Converter condition has been set to failed for the specified chassis, slot and socket.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterFailed		
Remedial action: Replace the failed power converter.		

Table 27-2898 IK8901130

Alarm	Attributes	Applicable major release
Name: IK8901130 (9447) Type: equipmentAlarm Package: lmg.IK8901130 Raised on class: lmg.FRU	Severity: warning Specific problem: Power Converter Redundancy Lost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The DC-DC Power Converters have lost redundancy for the specified chassis.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3PowerConverterRedundancyLost		
Remedial action: Check the power converters in the system for a failure in a redundant pair. Replace the power converter.		

Table 27-2899 IK8901131

Alarm	Attributes	Applicable major release
Name: IK8901131 (9448) Type: communicationsAlarm Package: lmg.IK8901131 Raised on class: lmg.FRU	Severity: minor Specific problem: Cache Accel Parity Errors may require a module Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.MG
Description: A cache accelerator parity error indicates a cache module needs to be replaced. The error information is reported in the variable cpqHeEventLogErrorDesc.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe3CacheAccelParityError		
Remedial action: Refer to the Integrated Management Log for details on the error. Replace the cache module.		

Table 27-2900 IK8901132

Alarm	Attributes	Applicable major release
Name: IK8901132 (9449) Type: processingErrorAlarm Package: Img.IK8901132 Raised on class: Img.FRU	Severity: warning Specific problem: Online Spare Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: Advanced Memory Protection Online Spare Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The Online Spare Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemOnlineSpareEngaged		
Remedial action: Schedule server down-time to replace the faulty memory.		

Table 27-2901 IK8901134

Alarm	Attributes	Applicable major release
Name: IK8901134 (9450) Type: equipmentAlarm Package: Img.IK8901134 Raised on class: Img.FRU	Severity: minor Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The fault tolerant power supply condition has been set to degraded for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2902 IK8901135

Alarm	Attributes	Applicable major release
Name: IK8901135 (8310) Type: equipmentAlarm Package: Img.IK8901135 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply condition has been set to failed for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2903 IK8901136

Alarm	Attributes	Applicable major release
Name: IK8901136 (9451) Type: processingErrorAlarm Package: Img.IK8901136 Raised on class: Img.FRU	Severity: warning Specific problem: Mirrored Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG

Table 27-2903 IK8901136 (continued)

Alarm	Attributes	Applicable major release
Description: Advanced Memory Protection Mirrored Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemMirroredMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2904 IK8901137

Alarm	Attributes	Applicable major release
Name: IK8901137 (9452) Type: processingErrorAlarm Package: lmg.IK8901137 Raised on class: lmg.FRU	Severity: warning Specific problem: Advanced ECC Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: Advanced Memory Protection Advanced ECC Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. Advanced ECC has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientAdvancedECCMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2905 IK8901138

Alarm	Attributes	Applicable major release
Name: IK8901138 (9453) Type: processingErrorAlarm Package: lmg.IK8901138 Raised on class: lmg.FRU	Severity: warning Specific problem: Advanced XOR Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: Advanced Memory Protection XOR Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The XOR engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemXorMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2906 IK8901142

Alarm	Attributes	Applicable major release
Name: IK8901142 (9454) Type: equipmentAlarm Package: lmg.IK8901142 Raised on class: lmg.FRU	Severity: warning Specific problem: Memory Board or Cartridge Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Memory board or cartridge removed. An Advanced Memory Protection sub-system board or cartridge has been removed from the system.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardRemoved		

Table 27-2906 IK8901142 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Insure the board or cartridge has memory correctly installed and re-insert the memory board or cartridge back into the system.		

Table 27-2907 IK8901144

Alarm	Attributes	Applicable major release
Name: IK8901144 (8311) Type: processingErrorAlarm Package: Img.IK8901144 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge bus error detected. An Advanced Memory Protection sub-system board or cartridge bus error has been detected.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge.		

Table 27-2908 IK8901148

Alarm	Attributes	Applicable major release
Name: IK8901148 (8312) Type: equipmentAlarm Package: Img.IK8901148 Raised on class: Img.FRU	Severity: major Specific problem: Management processor failed reset Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The Management processor failed reset The management processor was not successfully reset and is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeManagementProcFailedReset		
Remedial action: Reset the management procesessor again or re-flash the management processor firmware.		

Table 27-2909 IK8901150

Alarm	Attributes	Applicable major release
Name: IK8901150 (9455) Type: equipmentAlarm Package: Img.IK8901150 Raised on class: Img.FRU	Severity: warning Specific problem: Memory Board or Cartridge or Riser Removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Memory board or cartridge or riser removed. An Advanced Memory Protection sub-system board or cartridge or riser has been removed from the system. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardRemoved		
Remedial action: Insure the board or cartridge or riser has memory correctly installed and re-insert the memory board or cartridge or CPU back into the system.		

Table 27-2910 IK8901152

Alarm	Attributes	Applicable major release
Name: IK8901152 (8313) Type: processingErrorAlarm Package: Img.IK8901152 Raised on class: Img.FRU	Severity: major Specific problem: Memory Board or Cartridge or Riser Bus Error Detected Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG
Description: Memory board or cartridge or Riser bus error detected. An Advanced Memory Protection sub-system board or cartridge or Riser bus error has been detected. Value 0 for CPU means memory is not processor based.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHe5ResMemBoardBusError		
Remedial action: Replace the indicated board or cartridge or Riser.		

Table 27-2911 IK8901153

Alarm	Attributes	Applicable major release
Name: IK8901153 (9456) Type: processingErrorAlarm Package: Img.IK8901153 Raised on class: Img.FRU	Severity: warning Specific problem: Advanced LockStep Memory Engaged Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: Advanced Memory Protection LockStep Engine Memory Engaged. The Advanced Memory Protection subsystem has detected a memory fault. The LockStep engine has been activated.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHeResilientMemLockStepMemoryEngaged		
Remedial action: Replace the faulty memory.		

Table 27-2912 IK8901154

Alarm	Attributes	Applicable major release
Name: IK8901154 (8314) Type: equipmentAlarm Package: Img.IK8901154 Raised on class: Img.FRU	Severity: major Specific problem: Power Supply AC Power Loss Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The fault tolerant power supply AC power loss for the specified chassis and bay location.\nAlarm is cleared by the system.\nReason: cpqHe4FltTolPowerSupplyACpowerloss		
Remedial action: Check the power source for the specified power supply.		

Table 27-2913 IK8901156

Alarm	Attributes	Applicable major release
Name: IK8901156 (8315) Type: processingErrorAlarm Package: Img.IK8901156 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHoAppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2914 IK8901158

Alarm	Attributes	Applicable major release
Name: IK8901158 (8316) Type: processingErrorAlarm Package: Img.IK8901158 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Application Error Trap Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG
Description: An application has generated an exception. Specific error information is contained in the variable cpqHoSwPerfAppErrorDesc.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2AppErrorTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2915 IK8901160

Alarm	Attributes	Applicable major release
Name: IK8901160 (9457) Type: communicationsAlarm Package: Img.IK8901160 Raised on class: Img.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2916 IK8901163

Alarm	Attributes	Applicable major release
Name: IK8901163 (8317) Type: communicationsAlarm Package: lmg.IK8901163 Raised on class: lmg.FRU	Severity: major Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a NIC changes to the Failed condition.\nAlarm is cleared by the system.\nReason: cpqHo2NicStatusFailed2		
Remedial action: Check the network cables. Replace the failed NIC.		

Table 27-2917 IK8901164

Alarm	Attributes	Applicable major release
Name: IK8901164 (9458) Type: communicationsAlarm Package: lmg.IK8901164 Raised on class: lmg.FRU	Severity: warning Specific problem: Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time the configured redundant NIC becomes the active NIC.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHo2NicSwitchoverOccurred2		
Remedial action: Examine the network connections and check for a NIC failure.		

Table 27-2918 IK8901168

Alarm	Attributes	Applicable major release
Name: IK8901168 (9459) Type: processingErrorAlarm Package: lmg.IK8901168 Raised on class: lmg.FRU	Severity: warning Specific problem: Critical Software update Notification Trap Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.MG
Description: This alarm is a send to the user to notify him of a Critical Software Update.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqHoCriticalSoftwareUpdateTrap		
Remedial action: Install the required software updates.		

Table 27-2919 IK8901172

Alarm	Attributes	Applicable major release
Name: IK8901172 (8318) Type: qualityOfServiceAlarm Package: lmg.IK8901172 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Power Threshold Exceeded Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • LR14.3.MG
Description: This alarm notifies user of a power threshold breach. Power threshold exceeded.\nAlarm to be cleared by the operator at the management system.\nReason: cpqHo2PowerThresholdTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2920 IK8902265

Alarm	Attributes	Applicable major release
Name: IK8902265 (8319) Type: environmentalAlarm Package: lmg.IK8902265 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDaAccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2921 IK8902272

Alarm	Attributes	Applicable major release
Name: IK8902272 (8320) Type: environmentalAlarm Package: lmg.IK8902272 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa2AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2922 IK8902279

Alarm	Attributes	Applicable major release
Name: IK8902279 (8321) Type: environmentalAlarm Package: lmg.IK8902279 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board. The current battery status is indicated by the cpqDaAccelBattery variable.\nAlarm to be cleared by the operator at the management system.\nReason: cpqDa3AccelBatteryFailed		
Remedial action: check the Accelerator Board Battery		

Table 27-2923 IK8902281

Alarm	Attributes	Applicable major release
Name: IK8902281 (9460) Type: processingErrorAlarm Package: lmg.IK8902281 Raised on class: lmg.FRU	Severity: warning Specific problem: Duplex Controller Active Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.MG
Description: Controller Active. This alarm signifies that the agent has detected that a backup array controller in a duplexed pair has switched over to the active role. The variable cpqDaCntlrSlot indicates the active controller slot and cpqDaCntlrPartnerSlot indicates the backup.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDaCntlrActive		
Remedial action: Check the partner controller for problems. If this was the result of a user initiated switch over, no action is required.		

Table 27-2924 IK8902284

Alarm	Attributes	Applicable major release
Name: IK8902284 (9461) Type: equipmentAlarm Package: lmg.IK8902284 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa4PhyDrvThreshPassedTrap		
Remedial action: If the physical drive is predicting failure, replace the drive.		

Table 27-2925 IK8902291

Alarm	Attributes	Applicable major release
Name: IK8902291 (8322) Type: equipmentAlarm Package: lmg.IK8902291 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Bad Data. This alarm signifies that the agent has detected an array accelerator cache board that has lost battery power. If data was being stored in the accelerator cache memory when the server lost power, that data has been lost.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2926 IK8902292

Alarm	Attributes	Applicable major release
Name: IK8902292 (8323) Type: environmentalAlarm Package: lmg.IK8902292 Raised on class: lmg.FRU	Severity: major Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Accelerator Board Battery Failed. This alarm signifies that the agent has detected a battery failure associated with the array accelerator cache board.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa5AccelBatteryFailed		
Remedial action: Replace the Accelerator Cache Board.		

Table 27-2927 IK8902295

Alarm	Attributes	Applicable major release
Name: IK8902295 (8324) Type: equipmentAlarm Package: lmg.IK8902295 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa5PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2928 IK8902302

Alarm	Attributes	Applicable major release
Name: IK8902302 (8325) Type: equipmentAlarm Package: lmg.IK8902302 Raised on class: lmg.FRU	Severity: major Specific problem: Physical Drive Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Physical Drive Threshold Passed. This alarm signifies that the agent has detected a factory threshold associated with one of the physical drive objects on a drive array has been exceeded.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqDa6PhyDrvThreshPassedTrap		
Remedial action: Replace the physical drive.		

Table 27-2929 IK8902304

Alarm	Attributes	Applicable major release
Name: IK8902304 (9462) Type: equipmentAlarm Package: lmg.IK8902304 Raised on class: lmg.FRU	Severity: minor Specific problem: Accelerator Board Bad Data Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: Cache Module Board Bad Data. This alarm signifies that the agent has detected a cache module board that has lost backup power. If data was being stored in the cache module memory when the server lost power, that data has been lost. The backup power source is indicated by cpqDaAccelBackupPowerSource.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBadDataTrap		
Remedial action: Verify that no data has been lost.		

Table 27-2930 IK8902305

Alarm	Attributes	Applicable major release
Name: IK8902305 (9463) Type: environmentalAlarm Package: lmg.IK8902305 Raised on class: lmg.FRU	Severity: minor Specific problem: Accelerator Board Battery Failed Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR15.1.MG
Description: Cache Module Board Backup Power Source Failed. This alarm signifies that the agent has detected a backup power source failure associated with the cache module board. The backup power source is indicated by cpqDaAccelBackupPowerSource.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6AccelBatteryFailed		
Remedial action: Replace the Backup Power Source.		

Table 27-2931 IK8902309

Alarm	Attributes	Applicable major release
Name: IK8902309 (9464) Type: processingErrorAlarm Package: lmg.IK8902309 Raised on class: lmg.FRU	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-2932 IK8902310

Alarm	Attributes	Applicable major release
Name: IK8902310 (9465) Type: equipmentAlarm Package: lmg.IK8902310 Raised on class: lmg.FRU	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqDa6TapeDriveCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-2933 IK8902315

Alarm	Attributes	Applicable major release
Name: IK8902315 (9466) Type: equipmentAlarm Package: lmg.IK8902315 Raised on class: lmg.FRU	Severity: minor Specific problem: IDE Drive Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: An IDE drive status has been set to degraded.\nAlarm is cleared by the system.\nReason: cpqIdeDriveDegraded		
Remedial action: The drive should be scheduled for replacement. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-2934 IK8902317

Alarm	Attributes	Applicable major release
Name: IK8902317 (9467) Type: equipmentAlarm Package: lmg.IK8902317 Raised on class: lmg.FRU	Severity: minor Specific problem: IDE Drive Ultra ATA Degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: An IDE drive detects an excessive number of Ultra ATA data transmission errors between the hard drive and the processor.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqIdeDriveUltraAtaDegraded		
Remedial action: For best performance move Ultra ATA devices to the primary controller and non Ultra ATA devices to the secondary controller. If errors still persist, consider replacing the standard 40-conductor IDE cable with an 80-conductor Ultra ATA cable.		

Table 27-2935 IK8902337

Alarm	Attributes	Applicable major release
Name: IK8902337 (8326) Type: communicationsAlarm Package: lmg.IK8902337 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2936 IK8902339

Alarm	Attributes	Applicable major release
Name: IK8902339 (9468) Type: communicationsAlarm Package: lmg.IK8902339 Raised on class: lmg.FRU	Severity: minor Specific problem: NIC Status Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNicRedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2937 IK8902341

Alarm	Attributes	Applicable major release
Name: IK8902341 (8327) Type: communicationsAlarm Package: Img.IK8902341 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2938 IK8902343

Alarm	Attributes	Applicable major release
Name: IK8902343 (8328) Type: communicationsAlarm Package: Img.IK8902343 Raised on class: Img.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic2RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2939 IK8902347

Alarm	Attributes	Applicable major release
Name: IK8902347 (8329) Type: communicationsAlarm Package: Img.IK8902347 Raised on class: Img.FRU	Severity: major Specific problem: NIC Connectivity Lost Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time the status of a logical adapter changes to the Failed condition. This occurs when the adapter in a single adapter configuration fails, or when the last adapter in a redundant configuration fails. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNic3ConnectivityLost		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2940 IK8902349

Alarm	Attributes	Applicable major release
Name: IK8902349 (8330) Type: communicationsAlarm Package: lmg.IK8902349 Raised on class: lmg.FRU	Severity: major Specific problem: NIC Redundancy Reduced Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm will be sent any time a physical adapter in a logical adapter group changes to the Failed condition, but at least one physical adapter remains in the OK condition.. This can be caused by loss of link due to a cable being removed from the adapter or the Hub or Switch. Internal adapter, Hub, or Switch failures can also cause this condition.\nAlarm is cleared by the system.\nReason: cpqNic3RedundancyReduced		
Remedial action: Check the cables to the adapter and the Hub or Switch. If no cable problems are found, the adapter, Hub, or Switch may need replacement.		

Table 27-2941 IK8902360

Alarm	Attributes	Applicable major release
Name: IK8902360 (8331) Type: equipmentAlarm Package: lmg.IK8902360 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure temperature failed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure temperature status has been set to failed. This alarm signifies that a enclosure temperature sensor has been tripped indicating an overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempFailed		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-2942 IK8902361

Alarm	Attributes	Applicable major release
Name: IK8902361 (9469) Type: equipmentAlarm Package: lmg.IK8902361 Raised on class: lmg.FRU	Severity: minor Specific problem: Enclosure temperature degraded Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: The enclosure temperature status has been set to degraded. This alarm signifies that an enclosure temperature sensor has been tripped indicating a possible overheat condition.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureTempDegraded		
Remedial action: Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.		

Table 27-2943 IK8902363

Alarm	Attributes	Applicable major release
Name: IK8902363 (8332) Type: environmentalAlarm Package: lmg.IK8902363 Raised on class: lmg.FRU	Severity: major Specific problem: Enclosure fan failed Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR14.3.MG • LR15.1.MG
Description: The enclosure fan status has been set to failed. This alarm signifies that an enclosure fan has failed and no other fans in the redundant fan group are operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanFailed		
Remedial action: Replace the fan as soon as possible.		

Table 27-2944 IK8902364

Alarm	Attributes	Applicable major release
Name: IK8902364 (9470) Type: environmentalAlarm Package: lmg.IK8902364 Raised on class: lmg.FRU	Severity: minor Specific problem: Enclosure fan degraded Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The enclosure fan status has been set to degraded. This alarm signifies that an enclosure fan has failed but other fans in the redundant fan group are still operating. This may result in overheating of the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackEnclosureFanDegraded		
Remedial action: Replace the fan as soon as possible.		

Table 27-2945 IK8902368

Alarm	Attributes	Applicable major release
Name: IK8902368 (8333) Type: equipmentAlarm Package: lmg.IK8902368 Raised on class: lmg.FRU	Severity: critical Specific problem: Rack power supply failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to failed. This alarm signifies that a power supply has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyFailed		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2946 IK8902369

Alarm	Attributes	Applicable major release
Name: IK8902369 (8334) Type: equipmentAlarm Package: lmg.IK8902369 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The power supply status has been set to degraded. This alarm signifies that a power supply has degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSupplyDegraded		
Remedial action: Replace the power supply as soon as possible.		

Table 27-2947 IK8902373

Alarm	Attributes	Applicable major release
Name: IK8902373 (9471) Type: equipmentAlarm Package: lmg.IK8902373 Raised on class: lmg.FRU	Severity: minor Specific problem: Rack power subsystem not redundant Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The rack power subsystem is no longer in a redundant state.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemNotRedundant		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-2948 IK8902374

Alarm	Attributes	Applicable major release
Name: IK8902374 (8335) Type: equipmentAlarm Package: lmg.IK8902374 Raised on class: lmg.FRU	Severity: major Specific problem: Rack power supply input voltage problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power supply detected an input line voltage problem.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemLineVoltageProblem		
Remedial action: Check the power input for the power supply or replace any failed power supplies as soon as possible.		

Table 27-2949 IK8902375

Alarm	Attributes	Applicable major release
Name: IK8902375 (8336) Type: equipmentAlarm Package: Img.IK8902375 Raised on class: Img.FRU	Severity: major Specific problem: Rack power subsystem overload condition Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: The rack power subsystem overload condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerSubsystemOverloadCondition		
Remedial action: Replace any failed power supplies as soon as possible to return the system to a redundant state.		

Table 27-2950 IK8902376

Alarm	Attributes	Applicable major release
Name: IK8902376 (8337) Type: equipmentAlarm Package: Img.IK8902376 Raised on class: Img.FRU	Severity: critical Specific problem: Server shutdown due to power shedding Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server shutdown due to power shedding. The server blade was shutdown due to a lack of power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerShedAutoShutdown		
Remedial action: Check power connections or add power supplies.		

Table 27-2951 IK8902377

Alarm	Attributes	Applicable major release
Name: IK8902377 (8338) Type: equipmentAlarm Package: Img.IK8902377 Raised on class: Img.FRU	Severity: critical Specific problem: Server power on prevented to preserve redundancy Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server power on prevented to preserve redundancy. There is not enough power to power on the server blade and maintain redundancy for the other blades in the enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotRedundant		
Remedial action: Check power connections or add power supplies.		

Table 27-2952 IK8902378

Alarm	Attributes	Applicable major release
Name: IK8902378 (8339) Type: equipmentAlarm Package: Img.IK8902378 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailedNotEnoughPower		
Remedial action: Check power connections or add power supplies.		

Table 27-2953 IK8902379

Alarm	Attributes	Applicable major release
Name: IK8902379 (8340) Type: equipmentAlarm Package: Img.IK8902379 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The server enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFaile-dEnclosureNotFound		
Remedial action: Check server enclosure connections or add power supplies.		

Table 27-2954 IK8902380

Alarm	Attributes	Applicable major release
Name: IK8902380 (8341) Type: equipmentAlarm Package: Img.IK8902380 Raised on class: Img.FRU	Severity: critical Specific problem: Inadequate power to power on Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Inadequate power to power on. There is not enough power to power on the server blade. The power enclosure micro-controller was not found.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerPowerOnFailed-PowerChassisNotFound		
Remedial action: Check power enclosure connections or add power supplies.		

Table 27-2955 IK8902382

Alarm	Attributes	Applicable major release
Name: IK8902382 (8342) Type: environmentalAlarm Package: Img.IK8902382 Raised on class: Img.FRU	Severity: major Specific problem: Fuse open Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR14.3.MG • LR15.1.MG
Description: Fuse open. The fuse has been tripped.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackFuseOpen		
Remedial action: Check enclosure and / or blade power connections and reset the fuse.		

Table 27-2956 IK8902385

Alarm	Attributes	Applicable major release
Name: IK8902385 (9472) Type: equipmentAlarm Package: Img.IK8902385 Raised on class: Img.FRU	Severity: minor Specific problem: Power subsystem not load balanced Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: Power subsystem not load balanced. The power subsystem is out of balance for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisNotLoadBalanced		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies. Add additional power supplies if needed.		

Table 27-2957 IK8902386

Alarm	Attributes	Applicable major release
Name: IK8902386 (8343) Type: equipmentAlarm Package: Img.IK8902386 Raised on class: Img.FRU	Severity: major Specific problem: Power subsystem DC power problem Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem DC power problem. There is a power subsystem DC power problem for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisDcPowerProblem		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2958 IK8902387

Alarm	Attributes	Applicable major release
Name: IK8902387 (8344) Type: equipmentAlarm Package: lmg.IK8902387 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem AC facility input power exceeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem AC facility input power exceeded. There is a power subsystem Power subsystem AC facility input power exceeded for this power enclosure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisAc-FacilityPowerExceeded		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2959 IK8902388

Alarm	Attributes	Applicable major release
Name: IK8902388 (8345) Type: equipmentAlarm Package: lmg.IK8902388 Raised on class: lmg.FRU	Severity: major Specific problem: Unknown power consumption Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Unknown power consumption. There is an unknown power consumer drawing power.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerUnknownPowerConsumption		
Remedial action: Check the power enclosure and power supplies. Replace any failed or degraded power supplies.		

Table 27-2960 IK8902389

Alarm	Attributes	Applicable major release
Name: IK8902389 (9473) Type: equipmentAlarm Package: lmg.IK8902389 Raised on class: lmg.FRU	Severity: minor Specific problem: Power subsystem load balancing wire missing Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: Power subsystem load balancing wire missing. The power subsystem load balancing wire missing.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisLoadBalancingWireMissing		
Remedial action: Connect the load balancing wire.		

Table 27-2961 IK8902390

Alarm	Attributes	Applicable major release
Name: IK8902390 (9474) Type: equipmentAlarm Package: lmg.IK8902390 Raised on class: lmg.FRU	Severity: minor Specific problem: Power subsystem has too may power enclosures Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: Power subsystem has too may power enclosures. The maximum number of power enclosures has been exceeded.\ nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisTooManyPowerChassis		
Remedial action: Remove the extra power enclosure.		

Table 27-2962 IK8902391

Alarm	Attributes	Applicable major release
Name: IK8902391 (8346) Type: processingErrorAlarm Package: lmg.IK8902391 Raised on class: lmg.FRU	Severity: major Specific problem: Power subsystem improperly configured Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR14.3.MG • LR15.1.MG
Description: Power subsystem improperly configured. The power subsystem has been improperly configured.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerChassisConfigError		
Remedial action: Check the cabling of the power enclosure.		

Table 27-2963 IK8902392

Alarm	Attributes	Applicable major release
Name: IK8902392 (9475) Type: qualityOfServiceAlarm Package: lmg.IK8902392 Raised on class: lmg.FRU	Severity: minor Specific problem: Enclosure manager degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR15.1.MG
Description: The Onboard Administrator or other management processor status has been set to degraded. This alarm signifies that either an Onboard Administrator has failed but the other Onboard Administrator is still operating, or one or more management processors is in a non-optimal operating state.\nAlarm is cleared by the system.\nReason: cpqRackEnclosureManagerDegraded		
Remedial action: For C-Class enclosures, replace the Onboard Administrator as soon as possible. For all others please refer to product documenation for possible corrective actions		

Table 27-2964 IK8902401

Alarm	Attributes	Applicable major release
Name: IK8902401 (8347) Type: communicationsAlarm Package: lmg.IK8902401 Raised on class: lmg.FRU	Severity: critical Specific problem: Interconnect failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The interconnect status has been set to failed. This alarm signifies that a interconnect has failed.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorFailed		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-2965 IK8902402

Alarm	Attributes	Applicable major release
Name: IK8902402 (9476) Type: communicationsAlarm Package: lmg.IK8902402 Raised on class: lmg.FRU	Severity: minor Specific problem: Interconnect degraded Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: The interconnect status has been set to degraded. This alarm signifies that a interconnect has degraded.\nAlarm is cleared by the system.\nReason: cpqRackNetConnectorDegraded		
Remedial action: Replace the interconnect as soon as possible.		

Table 27-2966 IK8902408

Alarm	Attributes	Applicable major release
Name: IK8902408 (8348) Type: qualityOfServiceAlarm Package: lmg.IK8902408 Raised on class: lmg.FRU	Severity: major Specific problem: Server blade health status degraded Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Degraded. The server blade health status has changed to Degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeStatusDegraded		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2967 IK8902409

Alarm	Attributes	Applicable major release
Name: IK8902409 (8349) Type: processingErrorAlarm Package: Img.IK8902409 Raised on class: Img.FRU	Severity: critical Specific problem: Server blade health status critical Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade health status Critical. The server blade health status has changed to Critical.\nAlarm is cleared by the system.\nReason: cpqRackServerBladeStatusCritical		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2968 IK8902410

Alarm	Attributes	Applicable major release
Name: IK8902410 (9477) Type: equipmentAlarm Package: Img.IK8902410 Raised on class: Img.FRU	Severity: minor Specific problem: Server blade not responding to group capping requests Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: The server blade is not responding to the group capper. The server blade is not responding to capping requests from the enclosure group capper\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeGrpCapTimeout		
Remedial action: Reset the iLO management processor.		

Table 27-2969 IK8902411

Alarm	Attributes	Applicable major release
Name: IK8902411 (8350) Type: equipmentAlarm Package: Img.IK8902411 Raised on class: Img.FRU	Severity: major Specific problem: Server blade unexpected shutdown Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: Server blade shutdown unexpectadly. An unexpected shutdown event has occurred for this server blade.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeUnexpectedShutdown		
Remedial action: Check blade server and enclosure SYSLOG.		

Table 27-2970 IK8902428

Alarm	Attributes	Applicable major release
Name: IK8902428 (8351) Type: equipmentAlarm Package: Img.IK8902428 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic EAE Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG

Table 27-2970 IK8902428 (continued)

Alarm	Attributes	Applicable major release
Description: EAE Major trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackMajorEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2971 IK8902429

Alarm	Attributes	Applicable major release
Name: IK8902429 (8352) Type: equipmentAlarm Package: lmg.IK8902429 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Generic EAE Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: EAE Critical trap\nAlarm to be cleared by the operator at the management system.\nReason: cpqRackCriticalEAETrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2972 IK8902430

Alarm	Attributes	Applicable major release
Name: IK8902430 (9478) Type: equipmentAlarm Package: lmg.IK8902430 Raised on class: lmg.FRU	Severity: minor Specific problem: Generic Power Subsystem EAE Minor trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Minor trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMinorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2973 IK8902431

Alarm	Attributes	Applicable major release
Name: IK8902431 (8353) Type: equipmentAlarm Package: lmg.IK8902431 Raised on class: lmg.FRU	Severity: major Specific problem: Generic Power Subsystem EAE Major trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Major trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerMajorEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2974 IK8902432

Alarm	Attributes	Applicable major release
Name: IK8902432 (8354) Type: equipmentAlarm Package: Img.IK8902432 Raised on class: Img.FRU	Severity: critical Specific problem: Generic Power Subsystem EAE Critical trap Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: FlexFabric Cmdr Power Subsystem Critical trap.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackPowerCriticalEAETrap		
Remedial action: For FlexFabric Cmdr, please refer to product documentation for possible corrective actions.		

Table 27-2975 IK8902436

Alarm	Attributes	Applicable major release
Name: IK8902436 (8355) Type: equipmentAlarm Package: Img.IK8902436 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Generic WSMAN Major trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Major trap\nReason: cpqRackMajorWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2976 IK8902437

Alarm	Attributes	Applicable major release
Name: IK8902437 (8356) Type: equipmentAlarm Package: Img.IK8902437 Raised on class: Img.LMGMngElement	Severity: critical Specific problem: Generic WSMAN Critical trap Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • LR14.3.MG
Description: WSMAN Critical trap\nReason: cpqRackCriticalWSMANTrap		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2977 IK8902439

Alarm	Attributes	Applicable major release
Name: IK8902439 (8357) Type: communicationsAlarm Package: Img.IK8902439 Raised on class: Img.LMGMngElement	Severity: major Specific problem: Standby Recovery Server Interconnect Failure Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG

Table 27-2977 IK8902439 (continued)

Alarm	Attributes	Applicable major release
Description: Recovery Server serial interconnect failure. The Standby Recovery Agent reports that the local serial interconnect is not connected or has failed. The primary server is being shutdown in anticipation of the startup of the standby server.\nAlarm to be cleared by the operator at the management system.\nReason: cpqRsStandbyCableFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2978 IK8902443

Alarm	Attributes	Applicable major release
Name: IK8902443 (9479) Type: communicationsAlarm Package: lmg.IK8902443 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Device Connected Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapDeviceConnected		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-2979 IK8902444

Alarm	Attributes	Applicable major release
Name: IK8902444 (9480) Type: communicationsAlarm Package: lmg.IK8902444 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Connection Lost Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: A UPS device is reporting a Connection Lost due to one of the following. 1. The serial cable connected to the UPS has been unplugged. 2. The Network cable connected to the UPS has been unplugged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapConnectionLost		
Remedial action: Perform the following steps to clear the alarm: 1. Insure all cables are seated properly. 2. Check you network to insure it is functioning properly. 3. If the UPS is serially connected insure that the Serial Relay Agent is installed and running.		

Table 27-2980 IK8902462

Alarm	Attributes	Applicable major release
Name: IK8902462 (9481) Type: environmentalAlarm Package: Img.IK8902462 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Smoke Detected Implicitly cleared: true Default probable cause: smoke	Release: • LR15.1.MG
Description: A CMC device is reporting smoke detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCSmokeDetected		
Remedial action: Investigate CMC Device for an over temperature condition.		

Table 27-2981 IK8902464

Alarm	Attributes	Applicable major release
Name: IK8902464 (9482) Type: equipmentAlarm Package: Img.IK8902464 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Shock Detected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A CMC device is reporting shock detected.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCShockDetected		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2982 IK8902468

Alarm	Attributes	Applicable major release
Name: IK8902468 (9483) Type: equipmentAlarm Package: Img.IK8902468 Raised on class: Img.FRU	Severity: indeterminate Specific problem: CMC Aux 2 Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A CMC device has entered an alarm condition for auxiliary input 2.\nAlarm is cleared by the system.\nReason: cpqRPMTrapCMCAux2Alarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2983 IK8902490

Alarm	Attributes	Applicable major release
Name: IK8902490 (9484) Type: equipmentAlarm Package: Img.IK8902490 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS Input Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSInputVoltageNormal		

Table 27-2983 IK8902490 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-2984 IK8902493

Alarm	Attributes	Applicable major release
Name: IK8902493 (9485) Type: equipmentAlarm Package: lmg.IK8902493 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Output Voltage Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOutputVoltageNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-2985 IK8902494

Alarm	Attributes	Applicable major release
Name: IK8902494 (9486) Type: equipmentAlarm Package: lmg.IK8902494 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Output Overload Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting an overload condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSOutpu-tOverload		
Remedial action: Perform the following steps to clear the alarm: 1. Reduce the load on the UPS by moving some of the load to another UPS. 2. Consider moving to a larger UPS to support the current load.		

Table 27-2986 IK8902496

Alarm	Attributes	Applicable major release
Name: IK8902496 (9487) Type: environmentalAlarm Package: lmg.IK8902496 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Low Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR15.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryLow		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-2987 IK8902499

Alarm	Attributes	Applicable major release
Name: IK8902499 (9488) Type: equipmentAlarm Package: lmg.IK8902499 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Level Normal Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting low battery.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSBatteryLevelNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. When utility power is restored, charge the battery to it's full capacity. If the battery level continues to decrease, the UPS will not be able to sustain the output load!		

Table 27-2988 IK8902500

Alarm	Attributes	Applicable major release
Name: IK8902500 (9489) Type: equipmentAlarm Package: lmg.IK8902500 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS On Battery Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-2989 IK8902502

Alarm	Attributes	Applicable major release
Name: IK8902502 (9490) Type: equipmentAlarm Package: lmg.IK8902502 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS On Buck Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting an On Buck condition due to the following. 1. Utility power has increased above recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBuck		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2990 IK8902503

Alarm	Attributes	Applicable major release
Name: IK8902503 (9491) Type: equipmentAlarm Package: lmg.IK8902503 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS On Boost Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting an On Boost condition due to the following. 1. Utility power has dropped below recommended utility input levels.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnBoost		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-2991 IK8902504

Alarm	Attributes	Applicable major release
Name: IK8902504 (9492) Type: equipmentAlarm Package: lmg.IK8902504 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS On Utility Power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting on battery condition.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSOnUtilityPower		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load!		

Table 27-2992 IK8902507

Alarm	Attributes	Applicable major release
Name: IK8902507 (9493) Type: environmentalAlarm Package: lmg.IK8902507 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Temperature Normal Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSTemperatureNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-2993 IK8902508

Alarm	Attributes	Applicable major release
Name: IK8902508 (9494) Type: equipmentAlarm Package: lmg.IK8902508 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Internal Failure Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting a general UPS failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSInternal-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-2994 IK8902510

Alarm	Attributes	Applicable major release
Name: IK8902510 (9495) Type: environmentalAlarm Package: lmg.IK8902510 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR15.1.MG
Description: A UPS device is reporting a battery failure.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryFailure		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support. 3. Your battery may need to be replaced. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2995 IK8902512

Alarm	Attributes	Applicable major release
Name: IK8902512 (9496) Type: equipmentAlarm Package: lmg.IK8902512 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestFailed		
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2996 IK8902513

Alarm	Attributes	Applicable major release
Name: IK8902513 (9497) Type: equipmentAlarm Package: lmg.IK8902513 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS Diagnostic Test Succeeded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting a diagnostic test failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSDiagnosticTestSucceeded		
Remedial action: Perform the following steps to clear the alarm: 1. Your battery may need to be replaced. 2. If this error persists contact technical support. 3. The UPS may not be capable of supporting it's load if utility power fails!		

Table 27-2997 IK8902518

Alarm	Attributes	Applicable major release
Name: IK8902518 (9498) Type: equipmentAlarm Package: lmg.IK8902518 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Bypass Not Available Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting bypass not avaliable.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBypassNotAvailable		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-2998 IK8902522

Alarm	Attributes	Applicable major release
Name: IK8902522 (9499) Type: equipmentAlarm Package: lmg.IK8902522 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Utility Not Present Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: Indicates that the utility input is not present. This differs from alarm #57 in that the detected voltage is zero in this case.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSUtilityNotPresent		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-2999 IK8902526

Alarm	Attributes	Applicable major release
Name: IK8902526 (9500) Type: equipmentAlarm Package: Img.IK8902526 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringFault		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-3000 IK8902527

Alarm	Attributes	Applicable major release
Name: IK8902527 (9501) Type: equipmentAlarm Package: Img.IK8902527 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Site Wiring Fault Cleared Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting a fault in the input wiring, other than Phase Rotation: e.g., Ground/Neutral reversed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSSiteWiringNormal		
Remedial action: Perform the following steps to clear the alarm: 1. Contact an electrician.		

Table 27-3001 IK8902528

Alarm	Attributes	Applicable major release
Name: IK8902528 (9502) Type: equipmentAlarm Package: Img.IK8902528 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is no longer on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassOffManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-3002 IK8902529

Alarm	Attributes	Applicable major release
Name: IK8902529 (9503) Type: equipmentAlarm Package: lmg.IK8902529 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS is on manual bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is operating in manual bypass mode.\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqRPMtrapUPSBypassONManual		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-3003 IK8902531

Alarm	Attributes	Applicable major release
Name: IK8902531 (9504) Type: equipmentAlarm Package: lmg.IK8902531 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS was started without utility power Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device has been started while on battery power. AC input power is not present.\nAlarm is cleared by the system.\nReason: cppqRPMtrapUPSStartedOnBattery		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. If the UPS remains on battery for an extended time it will not be able to sustain the output load.		

Table 27-3004 IK8902533

Alarm	Attributes	Applicable major release
Name: IK8902533 (9505) Type: equipmentAlarm Package: lmg.IK8902533 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Input voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting input voltage is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSInput-OutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is plugged into an outlet supplied with utility power. 2. If the UPS remains on battery for an extended period of time it will not be able to sustain the load.		

Table 27-3005 IK8902534

Alarm	Attributes	Applicable major release
Name: IK8902534 (9506) Type: environmentalAlarm Package: Img.IK8902534 Raised on class: Img.FRU	Severity: indeterminate Specific problem: UPS temperature out of range Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: A UPS device is reporting temperature is out of range.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSTemperatureOutOfRange		
Remedial action: Perform the following steps to clear the alarm: 1. Check to make sure the UPS is in a well ventilated area. 2. Lower the ambient temperature in the area where the UPS is located.		

Table 27-3006 IK8902536

Alarm	Attributes	Applicable major release
Name: IK8902536 (9507) Type: equipmentAlarm Package: Img.IK8902536 Raised on class: Img.FRU	Severity: indeterminate Specific problem: The UPS is on automatic bypass Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is operating in auto bypass mode.\nAlarm is cleared by the system.\nReason: cpqRPMtrapUPSBypassOnAuto		
Remedial action: Perform the following steps to clear the alarm: 1. In bypass mode, the UPS cannot support devices if there is a power failure. 2. Once maintenance has been performed return the UPS to normal mode.		

Table 27-3007 IK8902538

Alarm	Attributes	Applicable major release
Name: IK8902538 (9508) Type: equipmentAlarm Package: Img.IK8902538 Raised on class: Img.FRU	Severity: indeterminate Specific problem: Output voltage is out of range Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting output voltage is out of Range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMtrapUPSOutputoutofRange		
Remedial action: Perform the following steps to clear the alarm: 1. Initiate a UPS self test. 2. If this error persists contact technical support.		

Table 27-3008 IK8902539

Alarm	Attributes	Applicable major release
Name: IK8902539 (9509) Type: equipmentAlarm Package: lmg.IK8902539 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: One or more UPS batteries have been disconnected Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting batteries are not connected to the UPS.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteriesDisconnected		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS Batteries. The UPS will not be capable of supporting it's load if the utility power fails!		

Table 27-3009 IK8902541

Alarm	Attributes	Applicable major release
Name: IK8902541 (9510) Type: environmentalAlarm Package: lmg.IK8902541 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS batteries are in a discharged condition Implicitly cleared: true Default probable cause: batteryDischarging	Release: • LR15.1.MG
Description: A UPS device is reporting batteries are completely discharged.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSBatteryDischarged		
Remedial action: Perform the following steps to clear the alarm: 1. Connect the UPS to utility power to charge the batteries. The UPS will not be able to support it's load if the utility power fails!		

Table 27-3010 IK8902543

Alarm	Attributes	Applicable major release
Name: IK8902543 (9511) Type: equipmentAlarm Package: lmg.IK8902543 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS circuit breaker needs attention Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A UPS device is reporting an output Breaker or Relay has failed or may be stuck open or closed with this alarm.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCheckBreaker		
Remedial action: Perform the following steps to clear the alarm: 1. Check all breakers on the UPS. 2. If this error persists contact technical support.		

Table 27-3011 IK8902545

Alarm	Attributes	Applicable major release
Name: IK8902545 (9512) Type: equipmentAlarm Package: lmg.IK8902545 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: Emergency Power Off activated Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting an Emergency Power Off (EPO) command has been received to shutdown the UPS immediately with out delay. This command may come from a local control panel or from a remote source.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRPMTrapUPSEPOInitiated		
Remedial action: Perform the following steps to clear the alarm: 1. Turn the UPS on to reapply power to attached equipment.		

Table 27-3012 IK8902546

Alarm	Attributes	Applicable major release
Name: IK8902546 (9513) Type: equipmentAlarm Package: lmg.IK8902546 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: UPS output has been manually turned off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The UPS has been powered off with user interaction.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSManualLoadDumped		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3013 IK8902548

Alarm	Attributes	Applicable major release
Name: IK8902548 (9514) Type: environmentalAlarm Package: lmg.IK8902548 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A cover panel has been removed Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.MG
Description: A UPS device is reporting a cover panel has been removed while utility power is present.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSCabinetDoorOpen		
Remedial action: Perform the following steps to clear the alarm: 1. Reinstall all panels. 2. If this error persists contact technical support.		

Table 27-3014 IK8902550

Alarm	Attributes	Applicable major release
Name: IK8902550 (9515) Type: environmentalAlarm Package: lmg.IK8902550 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS has encountered an fan failure Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: A UPS device is reporting a fan failure has occurred.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSFan-Failure		
Remedial action: Perform the following steps to clear the alarm: 1. If this error persists contact technical support.		

Table 27-3015 IK8902552

Alarm	Attributes	Applicable major release
Name: IK8902552 (9516) Type: processingErrorAlarm Package: lmg.IK8902552 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: The UPS N+1 load has been exceeded Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: A UPS device is reporting a loss of redundancy due to one of the following. 1. One or more of the Electronics Modules has failed 2. One or more of the electronics modules has been manually removed. 3. The amount of load on the UPS has increased to the point that the UPS is no longer able to support an N+1 configuration.\nAlarm is cleared by the system.\nReason: cpqRPMTrapUPSLos-sOfRedundancy		
Remedial action: Perform the following steps to clear the alarm: 1. Check the UPS to see if one of the modules has failed. 2. Make sure that all modules are securely plugged in. 3. Reduce the load to return the N+1 configuration. 4. If the amount of load is now going to exceed and N+1 configuration permanently, change the configuration on the front panel of the UPS to Capacity instead of Parallel N+1.		

Table 27-3016 IK8902554

Alarm	Attributes	Applicable major release
Name: IK8902554 (9517) Type: equipmentAlarm Package: lmg.IK8902554 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: A UPS shutdown is imminent Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting a shutdown imminent condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownImminent		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-3017 IK8902556

Alarm	Attributes	Applicable major release
Name: IK8902556 (9518) Type: equipmentAlarm Package: Img.IK8902556 Raised on class: Img.FRU	Severity: indeterminate Specific problem: A UPS shutdown is pending Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A UPS device is reporting shutdown pending condition.\nAlarm is cleared by the system.\nReason: cpqRPMTrap-UPSShutdownPending		
Remedial action: Perform the following steps to clear the alarm: 1. Immediately restore power to the UPS. The UPS will not continue to supply power to devices following the shutdown!		

Table 27-3018 IK8902559

Alarm	Attributes	Applicable major release
Name: IK8902559 (8358) Type: equipmentAlarm Package: Img.IK8902559 Raised on class: Img.FRU	Severity: critical Specific problem: Critical Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR14.3.MG • LR15.1.MG
Description: A critical alarm has occurred.\nAlarm is cleared by the system.\nReason: cpqPMTrapCritical		
Remedial action: Check the Trap Details for more information.		

Table 27-3019 IK8902560

Alarm	Attributes	Applicable major release
Name: IK8902560 (9519) Type: equipmentAlarm Package: Img.IK8902560 Raised on class: Img.FRU	Severity: warning Specific problem: Warning Alarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: A warning alarm has occurred.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqPMTrapWarning		
Remedial action: Check the Trap Details for more information.		

Table 27-3020 IK8902585

Alarm	Attributes	Applicable major release
Name: IK8902585 (9520) Type: processingErrorAlarm Package: Img.IK8902585 Raised on class: Img.FRU	Severity: warning Specific problem: Tape Drive Cleaning Required Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG

Table 27-3020 IK8902585 (continued)

Alarm	Attributes	Applicable major release
Description: Tape Drive Cleaning Required trap. The agent has detected a tape drive that needs to have a cleaning tape inserted and run. This will cause the tape drive heads to be cleaned.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleaningRequired		
Remedial action: Insert and run a cleaning tape in the tape drive.		

Table 27-3021 IK8902586

Alarm	Attributes	Applicable major release
Name: IK8902586 (9521) Type: equipmentAlarm Package: lmg.IK8902586 Raised on class: lmg.FRU	Severity: warning Specific problem: Tape Drive Cleaning Tape Needs Replacing Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Tape Drive Cleaning Tape Needs Replacing. The agent has detected that an autoloader tape unit has a cleaning tape that has been fully used and therefore needs to be replaced with a new cleaning tape.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3PhyDrvCleanTapeReplace		
Remedial action: Replace the cleaning tape.		

Table 27-3022 IK8902590

Alarm	Attributes	Applicable major release
Name: IK8902590 (9522) Type: environmentalAlarm Package: lmg.IK8902590 Raised on class: lmg.FRU	Severity: minor Specific problem: Tape Library Door Opened Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.MG
Description: Tape Library Door Open The agent has detected that the door on an autoloader is open so the unit is not operational.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqTape3LibraryDoorOpen		
Remedial action: Close the door on the tape library.		

Table 27-3023 IK8902606

Alarm	Attributes	Applicable major release
Name: IK8902606 (9523) Type: equipmentAlarm Package: lmg.IK8902606 Raised on class: lmg.FRU	Severity: warning Specific problem: System hood is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: System hood is removed. The hood status has been set to removed. The system's hood is not in a properly installed state. This situation may result in improper cooling of the system due to air flow changes caused by the missing hood.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHoodRemoved		

Table 27-3023 IK8902606 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the cover (hood), ensure the system's cover is properly installed. Verify the system is in working order.		

Table 27-3024 IK8902608

Alarm	Attributes	Applicable major release
Name: IK8902608 (9524) Type: environmentalAlarm Package: Img.IK8902608 Raised on class: Img.FRU	Severity: minor Specific problem: Monitor Condition Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: A fault reporting feature has exceeded normal limits for the monitor indicated by the cpqSiMonitorIndex. The monitor's condition is degraded due to the internal temperature exceeding normal operating limits. The monitor is still useable, but action should be taken to return the condition to OK.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionDegraded		
Remedial action: Physically check for obstructions to air flow around the monitor. Check the thermostat in the room that the system occupies. Allow the monitor to cool by turning off the monitor for 5 minutes then turn the monitor back on. After the monitor cools, another alarm indicating an improving condition, such as Monitor OK, will be issued.		

Table 27-3025 IK8902609

Alarm	Attributes	Applicable major release
Name: IK8902609 (8359) Type: processingErrorAlarm Package: Img.IK8902609 Raised on class: Img.FRU	Severity: major Specific problem: Monitor Condition Failed Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR14.3.MG • LR15.1.MG
Description: A fault reporting feature has exceeded normal limits in the monitor indicated by the cpqSiMonitorIndex. The monitor's condition has been set to failed due to an operational feature exceeding normal operating limits. The monitor will not be useable and should be replaced.\nAlarm is cleared by the system.\nReason: cpqSiMonitorConditionFailed		
Remedial action: Make a note of the monitor model number and serial number. Replace the monitor. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-3026 IK8902610

Alarm	Attributes	Applicable major release
Name: IK8902610 (8360) Type: processingErrorAlarm Package: Img.IK8902610 Raised on class: Img.FRU	Severity: major Specific problem: Excessive Correctable Memory Errors Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR14.3.MG • LR15.1.MG

Table 27-3026 IK8902610 (continued)

Alarm	Attributes	Applicable major release
Description: Correctable memory error count has exceeded the threshold for the memory module indicated by the 'cpqSiMemErrorIndex' variable. The appropriate cpqSiMemModuleECCStatus has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiCorrMemErrStatusDegraded		
Remedial action: For Desktops, the System Administrator should run the F10 Diagnostics on this system and select RAM LONG TEST. If it is determined that a module needs replacing, schedule maintenance for the system and replace the failed memory module. Refer to the appropriate Maintenance and Service Guide for detailed information on a component replacement.		

Table 27-3027 IK8902612

Alarm	Attributes	Applicable major release
Name: IK8902612 (9525) Type: processingErrorAlarm Package: lmg.IK8902612 Raised on class: lmg.FRU	Severity: warning Specific problem: Memory modules have changed Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: A memory configuration change has occurred. CpqSiMemConfigChangeData will indicate which memory modules slots have changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiMemConfigChange		
Remedial action: You may want to verify a valid reason for a memory configuration to have occurred. If system issuing the alert is a Desktop running NT, the memory configuration change information is also logged in the NT System Log.		

Table 27-3028 IK8902615

Alarm	Attributes	Applicable major release
Name: IK8902615 (8361) Type: equipmentAlarm Package: lmg.IK8902615 Raised on class: lmg.FRU	Severity: major Specific problem: Hot Plug Slot Board Failed Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Hot Plug Slot Board Failed Power-Up. A Hot Plug Slot Board has failed to power-up in the specified chassis and slot.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiHotPlugSlotPowerUpFailed		
Remedial action: Insure the board and all cables are installed correctly and the board type and revision are the same as the replaced board.		

Table 27-3029 IK8902616

Alarm	Attributes	Applicable major release
Name: IK8902616 (8362) Type: environmentalAlarm Package: lmg.IK8902616 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Failure Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR14.3.MG • LR15.1.MG

Table 27-3029 IK8902616 (continued)

Alarm	Attributes	Applicable major release
Description: The battery indicated by cpqSiSysBatteryIndex has failed and must be replaced.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryFailure		
Remedial action: Contact your System Administrator or Authorized Reseller to order a replacement battery. Recycle your old battery. For proper disposal information, refer to the documentation that came with your computer.		

Table 27-3030 IK8902617

Alarm	Attributes	Applicable major release
Name: IK8902617 (8363) Type: environmentalAlarm Package: lmg.IK8902617 Raised on class: lmg.FRU	Severity: major Specific problem: Battery Charging Degradation Implicitly cleared: true Default probable cause: lowBatteryThreshold	Release: • LR14.3.MG • LR15.1.MG
Description: Significant battery degradation has occurred with battery indicated by cpqSiSysBatteryIndex. The battery can no longer be fully recharged.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryChargingDegraded		
Remedial action: If using multiple batteries, run the Power Conservation Utility to identify the battery location. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-3031 IK8902618

Alarm	Attributes	Applicable major release
Name: IK8902618 (9526) Type: environmentalAlarm Package: lmg.IK8902618 Raised on class: lmg.FRU	Severity: warning Specific problem: Battery Calibration Error Implicitly cleared: true Default probable cause: batteryFailure	Release: • LR15.1.MG
Description: Calibration is needed with battery indicated by cpqSiSysBatteryIndex. The battery can not correctly indicate capacity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSiSysBatteryCalibrationError		
Remedial action: Run the Power Conservation Utility. Contact your System Administrator or Authorized Reseller to order a replacement battery.		

Table 27-3032 IK8902620

Alarm	Attributes	Applicable major release
Name: IK8902620 (8364) Type: equipmentAlarm Package: lmg.IK8902620 Raised on class: lmg.FRU	Severity: major Specific problem: Server Power Outage Implicitly cleared: true Default probable cause: powerProblem	Release: • LR14.3.MG • LR15.1.MG
Description: Server Power Outage. The Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSm2ServerPowerOutage		

Table 27-3032 IK8902620 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the server's power source.		

Table 27-3033 IK8902622

Alarm	Attributes	Applicable major release
Name: IK8902622 (8365) Type: environmentalAlarm Package: lmg.IK8902622 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Remote Insight Battery Failed Implicitly cleared: false Default probable cause: batteryFailure	Release: • LR14.3.MG
Description: Remote Insight Battery Failed. The Remote Insight battery has failed and needs to be replaced.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2BatteryFailed		
Remedial action: replace the failing Remote Insight battery.		

Table 27-3034 IK8902628

Alarm	Attributes	Applicable major release
Name: IK8902628 (8366) Type: equipmentAlarm Package: lmg.IK8902628 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: Remote Insight external power cable disconnected Implicitly cleared: false Default probable cause: powerProblem	Release: • LR14.3.MG
Description: External Power Cable Disconnected. The Remote Insight external power cable has been disconnected.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ExternalPowerCableDisconnected		
Remedial action: check External Power Cable		

Table 27-3035 IK8902632

Alarm	Attributes	Applicable major release
Name: IK8902632 (8367) Type: processingErrorAlarm Package: lmg.IK8902632 Raised on class: lmg.LMGMngElement	Severity: critical Specific problem: Server Fatal Error Detected Implicitly cleared: false Default probable cause: softwareError	Release: • LR14.3.MG
Description: Server Fatal Error Detected. The Remote Insight/ Integrated Lights-Out firmware has detected a server fatal error.\nAlarm to be cleared by the operator at the management system.\nReason: cpqSm2ServerFatalError		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3036 IK8902633

Alarm	Attributes	Applicable major release
Name: IK8902633 (8368) Type: communicationsAlarm Package: lmg.IK8902633 Raised on class: lmg.FRU	Severity: major Specific problem: The iLO NIC Link is Down Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG • LR15.1.MG
Description: The iLO NIC Link is Down. The Remote Insight/ Integrated Lights-Out firmware has detected the loss of network link.\nAlarm is cleared by the system.\nReason: cpqSm2NicLinkDown		
Remedial action: Check the network connections for the iLO.		

Table 27-3037 IK8902636

Alarm	Attributes	Applicable major release
Name: IK8902636 (9527) Type: equipmentAlarm Package: lmg.IK8902636 Raised on class: lmg.FRU	Severity: major Specific problem: Server powered off Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The server has been powered off. This will be sent once the server has been powered off, either by OS, or the power button.\nAlarm is cleared by the system.\nReason: cpqSm2ServerPowerOff		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3038 IK8902647

Alarm	Attributes	Applicable major release
Name: IK8902647 (9528) Type: qualityOfServiceAlarm Package: lmg.IK8902647 Raised on class: lmg.FRU	Severity: minor Specific problem: PC Card Thermal Degraded Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for safe operations thereby causing degraded operations. This alarm will be sent when cpqSePCCardStatus transitions from Normal (1) to Thermal Degraded (2). The manufacturer and product information strings as well as the slot number for the degraded PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalDegraded		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3039 IK8902648

Alarm	Attributes	Applicable major release
Name: IK8902648 (8369) Type: qualityOfServiceAlarm Package: lmg.IK8902648 Raised on class: lmg.FRU	Severity: major Specific problem: PC Card Thermal Failure Status Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR14.3.MG • LR15.1.MG
Description: This alarm is sent when the PC Card Slot Thermal Sensor threshold has been exceeded for degraded operations thereby causing failed operations. This alarm will be sent when cpqSePCCardStatus transitions from Thermal Degraded (2) to Thermal Failure (3). The manufacturer and product information strings as well as the slot number for the failed PC Card is provided as parameters for this trap.\nAlarm is cleared by the system.\nReason: cpqSePCCardThermalFailure		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3040 IK8902657

Alarm	Attributes	Applicable major release
Name: IK8902657 (8370) Type: environmentalAlarm Package: lmg.IK8902657 Raised on class: lmg.FRU	Severity: major Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR14.3.MG • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system.\nReason: cpqSsTempFailed		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3041 IK8902658

Alarm	Attributes	Applicable major release
Name: IK8902658 (9529) Type: environmentalAlarm Package: lmg.IK8902658 Raised on class: lmg.FRU	Severity: minor Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system.\nReason: cpqSsTempDegraded		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3042 IK8902661

Alarm	Attributes	Applicable major release
Name: IK8902661 (9530) Type: equipmentAlarm Package: Img.IK8902661 Raised on class: Img.FRU	Severity: minor Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system.\nReason: cpqSsSidePanelRemoved		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3043 IK8902664

Alarm	Attributes	Applicable major release
Name: IK8902664 (9531) Type: environmentalAlarm Package: Img.IK8902664 Raised on class: Img.FRU	Severity: warning Specific problem: Storage System Temperature Failure Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: Storage System temperature failure. The agent has detected that a temperature status has been set to failed. The storage system will be shutdown.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempFailed		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-3044 IK8902665

Alarm	Attributes	Applicable major release
Name: IK8902665 (9532) Type: environmentalAlarm Package: Img.IK8902665 Raised on class: Img.FRU	Severity: warning Specific problem: Storage System Temp Degraded Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: Storage System temperature degraded. The agent has detected a temperature status that has been set to degraded. The storage system's temperature is outside of the normal operating range.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3TempDegraded		
Remedial action: Shutdown the storage system as soon as possible. Insure that the storage system environment is being cooled properly and that no components are overheated.		

Table 27-3045 IK8902668

Alarm	Attributes	Applicable major release
Name: IK8902668 (9533) Type: equipmentAlarm Package: lmg.IK8902668 Raised on class: lmg.FRU	Severity: warning Specific problem: Storage System side panel is removed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Storage System side panel is removed. The side panel status has been set to removed. The storage system's side panel is not in a properly installed state. This situation may result in improper cooling of the drives in the storage system due to air flow changes caused by the missing side panel.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs3SidePanelRemoved		
Remedial action: Replace the storage system side panel.		

Table 27-3046 IK8902670

Alarm	Attributes	Applicable major release
Name: IK8902670 (9534) Type: equipmentAlarm Package: lmg.IK8902670 Raised on class: lmg.FRU	Severity: warning Specific problem: Power Supply Degraded Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: A storage system power supply status has been set to degraded.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqSs4PwrSupplyDegraded		
Remedial action: Take action to restore power or replace any failed storage system power supply.		

Table 27-3047 IK8902695

Alarm	Attributes	Applicable major release
Name: IK8902695 (9535) Type: equipmentAlarm Package: lmg.IK8902695 Raised on class: lmg.FRU	Severity: minor Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMeRisingAlarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3048 IK8902697

Alarm	Attributes	Applicable major release
Name: IK8902697 (9536) Type: equipmentAlarm Package: lmg.IK8902697 Raised on class: lmg.FRU	Severity: warning Specific problem: Rising Threshold Passed Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Rising Threshold passed. An alarm entry has crossed its rising threshold. The instances of those objects contained within the variable list are those of the alarm entry which generated this trap.\nAlarm is cleared by the system.\nReason: cpqMe2RisingAlarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3049 IK8902748

Alarm	Attributes	Applicable major release
Name: IK8902748 (9537) Type: equipmentAlarm Package: lmg.IK8902748 Raised on class: lmg.FRU	Severity: indeterminate Specific problem: fluteModuleAlarm Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.MG
Description: Alarm notification\nAlarm is cleared by the system.\nReason: fluteModuleAlarm		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3050 IK8904762

Alarm	Attributes	Applicable major release
Name: IK8904762 (8371) Type: communicationsAlarm Package: lmg.IK8904762 Raised on class: lmg.LMGMngElement	Severity: major Specific problem: linkDown Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR14.3.MG
Description: A linkDown alarm signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.\nAlarm is cleared by the system.\nReason: linkDown		
Remedial action: If the problem persists, contact Nokia customer support.		

Table 27-3051 IK8907456

Alarm	Attributes	Applicable major release
Name: IK8907456 (9538) Type: environmentalAlarm Package: lmg.IK8907456 Raised on class: lmg.FRU	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG

Table 27-3051 IK8907456 (continued)

Alarm	Attributes	Applicable major release
Description: The temperature at rack sensor 1 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp1		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-3052 IK8907457

Alarm	Attributes	Applicable major release
Name: IK8907457 (9539) Type: environmentalAlarm Package: lmg.IK8907457 Raised on class: lmg.FRU	Severity: warning Specific problem: Temperature-alarm Implicitly cleared: true Default probable cause: temperatureUnacceptable	Release: • LR15.1.MG
Description: The temperature at rack sensor 2 is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmTemp2		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-3053 IK8907458

Alarm	Attributes	Applicable major release
Name: IK8907458 (9540) Type: environmentalAlarm Package: lmg.IK8907458 Raised on class: lmg.FRU	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The status of Fan 1 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan1		
Remedial action: Refer to Trap Details for more information.		

Table 27-3054 IK8907459

Alarm	Attributes	Applicable major release
Name: IK8907459 (9541) Type: environmentalAlarm Package: lmg.IK8907459 Raised on class: lmg.FRU	Severity: warning Specific problem: Fan-alarm Implicitly cleared: true Default probable cause: coolingFanFailure	Release: • LR15.1.MG
Description: The status of Fan 2 has changed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmFan2		
Remedial action: Refer to Trap Details for more information.		

Table 27-3055 IK8907460

Alarm	Attributes	Applicable major release
Name: IK8907460 (9542) Type: equipmentAlarm Package: Img.IK8907460 Raised on class: Img.FRU	Severity: warning Specific problem: Voltage-alarm Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.MG
Description: The AC voltage of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmVoltage		
Remedial action: Check the incoming power source and ensure all cables are inserted correctly.		

Table 27-3056 IK8907461

Alarm	Attributes	Applicable major release
Name: IK8907461 (9543) Type: environmentalAlarm Package: Img.IK8907461 Raised on class: Img.FRU	Severity: warning Specific problem: Humidity-alarm Implicitly cleared: true Default probable cause: humidityUnacceptable	Release: • LR15.1.MG
Description: The humidity of the rack is outside the specified threshold.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmHumidity		
Remedial action: Check the air handling system for the rack and refer to Trap Details for more information.		

Table 27-3057 IK8907462

Alarm	Attributes	Applicable major release
Name: IK8907462 (9544) Type: environmentalAlarm Package: Img.IK8907462 Raised on class: Img.FRU	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG
Description: The door or sidepanel of the rack has been opened (access point #1).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput1		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3058 IK8907463

Alarm	Attributes	Applicable major release
Name: IK8907463 (9545) Type: environmentalAlarm Package: Img.IK8907463 Raised on class: Img.FRU	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG

Table 27-3058 IK8907463 (continued)

Alarm	Attributes	Applicable major release
Description: The door or sidepanel of the rack has been opened (access point #2).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput2		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3059 IK8907464

Alarm	Attributes	Applicable major release
Name: IK8907464 (9546) Type: environmentalAlarm Package: lmg.IK8907464 Raised on class: lmg.FRU	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG
Description: The door or sidepanel of the rack has been opened (access point #3).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput3		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3060 IK8907465

Alarm	Attributes	Applicable major release
Name: IK8907465 (9547) Type: environmentalAlarm Package: lmg.IK8907465 Raised on class: lmg.FRU	Severity: warning Specific problem: Door/sidepanel-alarm Implicitly cleared: true Default probable cause: intrusionDetection	Release: • LR15.1.MG
Description: The door or sidepanel of the rack has been opened (access point #4).\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmInput4		
Remedial action: Check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3061 IK8907466

Alarm	Attributes	Applicable major release
Name: IK8907466 (9548) Type: processingErrorAlarm Package: lmg.IK8907466 Raised on class: lmg.FRU	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: Rack door lock #1 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3062 IK8907467

Alarm	Attributes	Applicable major release
Name: IK8907467 (9549) Type: processingErrorAlarm Package: lmg.IK8907467 Raised on class: lmg.FRU	Severity: warning Specific problem: Door-locking-alarm Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: Rack door lock #2 alarm.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2		
Remedial action: Ensure the door is completely closed and check for unauthorized intrusion and refer to Trap Details for more information.		

Table 27-3063 IK8907468

Alarm	Attributes	Applicable major release
Name: IK8907468 (9550) Type: environmentalAlarm Package: lmg.IK8907468 Raised on class: lmg.FRU	Severity: warning Specific problem: Smoke-alarm Implicitly cleared: true Default probable cause: smoke	Release: • LR15.1.MG
Description: The rack smoke detector has detected smoke.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmSmoke		
Remedial action: Investigate rack for an over temperature condition and refer to Trap Details for more information.		

Table 27-3064 IK8907469

Alarm	Attributes	Applicable major release
Name: IK8907469 (9551) Type: environmentalAlarm Package: lmg.IK8907469 Raised on class: lmg.FRU	Severity: warning Specific problem: Shock-alarm Implicitly cleared: true Default probable cause: excessiveVibration	Release: • LR15.1.MG
Description: The rack shock detector has detected a vibration to the rack.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmShock		
Remedial action: Investigate rack.		

Table 27-3065 IK8907474

Alarm	Attributes	Applicable major release
Name: IK8907474 (9552) Type: processingErrorAlarm Package: lmg.IK8907474 Raised on class: lmg.FRU	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: The rack door locking device #1 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock1Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-3066 IK8907475

Alarm	Attributes	Applicable major release
Name: IK8907475 (9553) Type: processingErrorAlarm Package: lmg.IK8907475 Raised on class: lmg.FRU	Severity: warning Specific problem: Door-locking-alarm of device Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.MG
Description: The rack door locking device #2 has failed.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqCmcalarmLock2Dev		
Remedial action: Check the device lock cable or failed battery and refer to Trap Details for more information.		

Table 27-3067 IK8907477

Alarm	Attributes	Applicable major release
Name: IK8907477 (9554) Type: processingErrorAlarm Package: lmg.IK8907477 Raised on class: lmg.FRU	Severity: warning Specific problem: Corrected - uncorrectable Memory Errors - Replace Memory Module Implicitly cleared: true Default probable cause: memoryMismatch	Release: • LR15.1.MG
Description: Corrected - uncorrected Memory Errors Detected The errors have been corrected, but the memory module should be replaced. Value 0 for CPU means memory is not Processor based\nAlarm is cleared by the system when the device is restarted.\ nReason: cpqHe5CorrMemReplaceMemModule		
Remedial action: Replace the failing memory module.		

Table 27-3068 IK8907478

Alarm	Attributes	Applicable major release
Name: IK8907478 (9555) Type: communicationsAlarm Package: Img.IK8907478 Raised on class: Img.FRU	Severity: warning Specific problem: NIC Virus-like Activity Detected Trap Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: This alarm will be sent when the Virus Throttle Filter Driver detects virus like activity.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqNicVirusLikeActivityDetected		
Remedial action: The system reporting this trap requires immediate attention.		

Table 27-3069 IK8907479

Alarm	Attributes	Applicable major release
Name: IK8907479 (9556) Type: communicationsAlarm Package: Img.IK8907479 Raised on class: Img.FRU	Severity: minor Specific problem: Server Blade e-keying failed Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.MG
Description: The server blade e-keying has failed. This alarm signifies that a server blade e-keying has failed and there is a port mapping problem between a server mezz card and the interconnect.\nAlarm is cleared by the system when the device is restarted.\nReason: cpqRackServerBladeEKeyingFailed		
Remedial action: Reconfigure server blade mezz cards.		

Table 27-3070 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 27-3071 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 27-3072 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 27-3073 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 27-3073 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 27-3074 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 27-3075 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 27-3076 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 27-3077 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 27-3078 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 27-3079 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 27-3080 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 27-3081 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		

Table 27-3081 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 27-3082 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 27-3083 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 27-3084 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 27-3085 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 27-3086 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 27-3086 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 27-3087 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 27-3088 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 27-3089 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 27-3090 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 27-3091 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 27-3091 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 27-3092 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 27-3093 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 27-3093 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 27-3094 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 27-3095 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG

Table 27-3095 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 27-3096 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 27-3097 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 27-3098 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 27-3099 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 27-3100 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 27-3101 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 27-3102 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • LR14.3.MG • LR15.1.MG • LR16.1.MG
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

28 9966 SC GW

28.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 28-1 AAA_addressPoolExhausted

Alarm	Attributes	Applicable major release
Name: AAA_addressPoolExhausted (5673) Type: qualityOfServiceAlarm Package: femto.AAA_addressPoolExhausted Raised on class: femto.AAA	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the address pool for the available SeGW servers has become exhausted		
Remedial action: The AAA_addressPoolExhausted alarm is raised when all IPs in the VPN-IP pool are allocated. When the RADIUS Access request message is received, the Nas IP, Nas Id, Nas Port and the called Station Id is searched in the SecurityGateway MO Class. cd /opt/bin./BSGCLI.execd FGW:<DN Number>;cd AAA:<DN Number>;cd securityGateway:<DN Number>;get securityGateway-FemtoVPNSubnets;The returned range is exhausted.When the lease time expires, AAA server sends an Accounting-Stop message to SeGW and the VPN-IP state is set as Reserved. cd /opt/bin./BSGCLI.execd FGW:<DN Number>;cd AAA:<DN Number>;cd securityGateway:<DN Number>;get securityGatewayAddressLeaseTime;The returned range is exhausted.On receiving an Accounting-Response message from Security Gateway, or when an Accounting-Stop message is retried until AAA::maxAcctReqXmts limit is reached, the VPN IP state changes to Available. cd /opt/bin./BSGCLI.execd FGW:<DN Number>;cd AAA:<DN Number>;get maxAcctReqXmts;		

Table 28-2 AAA_centralAAAFailure

Alarm	Attributes	Applicable major release
Name: AAA_centralAAAFailure (5674) Type: communicationsAlarm Package: femto.AAA_centralAAAFailure Raised on class: femto.AAA	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when communication to all central AAA has failed.		

Table 28-2 AAA_centralAAAFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: This fault is generated when the BSR Gateway is unable to establish connection with any of the configured remote AAA servers. cd /opt/bin./BSGCLI.execd FGW:<DN Number>;cd AAA:<DN Number>;cd AAAremoteAAAServer:<DN Number>;get remoteAAAServerIpAddress;A maximum of 10 remote AAA servers can be configured. Run Wireshark in BSR Gateway. Check whether RADIUS Access-Request message is forwarded to any one of the configured Remote AAA servers. Ping each configured remote AAA server's IP address (remoteAAAServerIpAddress) and check for any connectivity issues.		

Table 28-3 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 28-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 28-5 AGPSProxy_agpsServiceFailure

Alarm	Attributes	Applicable major release
Name: AGPSProxy_agpsServiceFailure (5675) Type: communicationsAlarm Package: femto.AGPSProxy_agpsServiceFailure Raised on class: femto.AGPSProxy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is raised if a failure is detected on the Assisted GPS Service		
Remedial action: This alarm is cleared automatically from the OAM system.		

Table 28-6 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 28-7 AMCSlot_deviceInstalledAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_deviceInstalledAssert (5679) Type: equipmentAlarm Package: femto.AMCSlot_deviceInstalledAssert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Device installed assert		
Remedial action: The operator must do a manual clearance.		

Table 28-8 AMCSlot_deviceInstalledDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_deviceInstalledDeassert (5680) Type: equipmentAlarm Package: femto.AMCSlot_deviceInstalledDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Device installed deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-9 AMCSlot_ds75DeviceinstalledCriticalAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledCriticalAssert (5681) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledCriticalAssert Raised on class: femto.AMCSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed critical assert		
Remedial action: No action needed. Indicates device is being installed.		

Table 28-10 AMCSlot_ds75DeviceinstalledCriticalDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledCriticalDeassert (5682) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledCriticalDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed critical deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-11 AMCSlot_ds75DeviceinstalledMajorAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledMajorAssert (5683) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledMajorAssert Raised on class: femto.AMCSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed major assert		
Remedial action: No action needed. Indicates device is being installed.		

Table 28-12 AMCSlot_ds75DeviceinstalledMajorDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledMajorDeassert (5684) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledMajorDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed major deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-13 AMCSlot_ds75DeviceinstalledMinorAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledMinorAssert (5685) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledMinorAssert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed minor assert		
Remedial action: The operator must do a manual clearance.		

Table 28-14 AMCSlot_ds75DeviceinstalledMinorDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_ds75DeviceinstalledMinorDeassert (5686) Type: equipmentAlarm Package: femto.AMCSlot_ds75DeviceinstalledMinorDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: DS 75 device installed minor deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-15 AMCSlot_info12vDeviceInstalledAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info12vDeviceInstalledAssert (5687) Type: equipmentAlarm Package: femto.AMCSlot_info12vDeviceInstalledAssert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 12V device installed assert		
Remedial action: The operator must do a manual clearance.		

Table 28-16 AMCSlot_info12vDeviceInstalledDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info12vDeviceInstalledDeassert (5688) Type: equipmentAlarm Package: femto.AMCSlot_info12vDeviceInstalledDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 12v device installed deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-17 AMCSlot_info3vDeviceInstalledAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info3vDeviceInstalledAssert (5689) Type: equipmentAlarm Package: femto.AMCSlot_info3vDeviceInstalledAssert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 3V device installed assert		
Remedial action: The operator must do a manual clearance.		

Table 28-18 AMCSlot_info3vDeviceInstalledDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info3vDeviceInstalledDeassert (5690) Type: equipmentAlarm Package: femto.AMCSlot_ info3vDeviceInstalledDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 3v device installed deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-19 AMCSlot_info5vDeviceInstalledAssert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info5vDeviceInstalledAssert (5691) Type: equipmentAlarm Package: femto.AMCSlot_info5vDeviceInstalledAssert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 5V device installed assert		
Remedial action: The operator must do a manual clearance.		

Table 28-20 AMCSlot_info5vDeviceInstalledDeassert

Alarm	Attributes	Applicable major release
Name: AMCSlot_info5vDeviceInstalledDeassert (5692) Type: equipmentAlarm Package: femto.AMCSlot_ info5vDeviceInstalledDeassert Raised on class: femto.AMCSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: 5V device installed deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-21 Application4G_droppingS1Traffic

Alarm	Attributes	Applicable major release
Name: Application4G_droppingS1Traffic (5693) Type: qualityOfServiceAlarm Package: femto.Application4G_droppingS1Traffic Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW drops S1 traffic since SCGW CPU/Memory utilization has crossed maximum threshold		
Remedial action: The alarm is cleared when the BSR Gateway recovers from the overload condition.The %CPU column of top command can be used to check the CPU utilization.Enter the command free to check the memory utilization.Free memory specified should be high. compared to the used memory available, for recovering to normal overload.The used buffer cache memory should be low.To drop the cache memory use the command echo 3 >/proc/sys/vm/drop_caches.Terminate some calls to check whether memory utilization comes down, clearing the alarm.If the memory utilization does not reduce and the alarm persists, de-register the Small Cells and check for reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforced Small Cell de-registration. Enforce a BSR Gateway switch-over by terminating the BSR Gateway application.		

Table 28-22 Application4G_dSMessageQueueOverloadMaximumThreshold

Alarm	Attributes	Applicable major release
Name: Application4G_ dSMessageQueueOverloadMaximumThreshold (12955) Type: equipmentAlarm Package: femto.Application4G_ dSMessageQueueOverloadMaximumThreshold Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfMessageQueue	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the maximum message queue overload threshold has been exceeded for the DS process.		

Table 28-22 Application4G_dSMessageQueueOverloadMaximumThreshold (continued)

Alarm	Attributes	Applicable major release
Remedial action: The FGW may initiate a failover to the available standby FGW if CPU or Memory maximum thresolds also get exceeded along with DS message queue threshold. If significant detoriation in KPIs is seen perform forceful FGW switch-over manually.For further assistance please contact NOKIA customer support.		

Table 28-23 Application4G_dSMessageQueueOverloadMinimumThreshold

Alarm	Attributes	Applicable major release
Name: Application4G_ dSMessageQueueOverloadMinimumThreshold (12956) Type: equipmentAlarm Package: femto.Application4G_ dSMessageQueueOverloadMinimumThreshold Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the minimum message queue overload threshold has been exceeded for the DS process.		
Remedial action: This alarm is cleared when either the measured DS process main message queues usage falls below the minimum threshold or rises above the maximum threshold.If the alarm persists for a long duration and not cleared on its own, terminate some calls and check whether message queue utilization comes down and the alarm is cleared.If message queue utilization does not come down and alarm is still present, de-register the Small Cells in a phased manner and check whether queue utilization comes down.For further assistance please contact NOKIA customer support.		

Table 28-24 Application4G_failedToDecodeMMESentMsg

Alarm	Attributes	Applicable major release
Name: Application4G_failedToDecodeMMESentMsg (5694) Type: communicationsAlarm Package: femto.Application4G_ failedToDecodeMMESentMsg Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is triggered when SCGW fails to decode messages sent by MME		
Remedial action: Check whether the messages from the MME are properly framed.This is MME message encoding problem or 3GPP release version support mismatchbetween FGW and MME.This fault is cleared manually from the OAM system.		

Table 28-25 Application4G_failedToSendDataToHeNB

Alarm	Attributes	Applicable major release
Name: Application4G_failedToSendDataToHeNB (5695) Type: communicationsAlarm Package: femto.Application4G_ failedToSendDataToHeNB Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW fails to send data to BSR		
Remedial action: Check the connectivity between the Small Cell and BSR Gateway.Check whether the BSR Gateway sctp port (6005) towards Small Cell is open.Check for any errors with respect to sending the data towards Small Cell. This can be done by looking for LOG ERROR statements in LOG_FMG.log file under /opt/log/.Use the above mentioned information to isolate the issue at Small Cell or BSR Gateway.This alarm is cleared when data from the BSR Gateway reaches the Small Cell successfully.		

Table 28-26 Application4G_failedToSendDataToMME

Alarm	Attributes	Applicable major release
Name: Application4G_failedToSendDataToMME (5696) Type: communicationsAlarm Package: femto.Application4G_ failedToSendDataToMME Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW fails to send data to MME		
Remedial action: Reduce memory utilization in SCGW, using the command free. Check if there is a reduction.Check whether memory overload alarm has been triggered.Terminate some calls to check if the memory utilization reduces, clearing the alarm.If there is no reduction in memory utilization, and the overload alarm still persists, then de-register the Small Cells. Now check for any reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforced Small Cell de-registration. Enforce a BSR Gateway switchover by terminating the BSR Gateway application		

Table 28-27 Application4G_henBGrpMessageQueueOverloadMaximumThreshold

Alarm	Attributes	Applicable major release
Name: Application4G_ henBGrpMessageQueueOverloadMaximumThreshold (12957) Type: equipmentAlarm Package: femto.Application4G_ henBGrpMessageQueueOverloadMaximumThreshold Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfMessageQueue	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the maximum message queue overload threshold has been exceeded for the HeNBGroup processes.		

Table 28-27 Application4G_henBGrpMessageQueueOverloadMaximumThreshold (continued)

Alarm	Attributes	Applicable major release
Remedial action: The FGW may initiate a failover to the available standby FGW if CPU or Memory maximum thresolds also get exceeded along with HeNBGrps message queue threshold.If significant detoriation in KPIs is seen perform forceful FGW switch-over manually.For further assistance please contact NOKIA customer support.		

Table 28-28 Application4G_henBGrpMessageQueueOverloadMinimumThreshold

Alarm	Attributes	Applicable major release
Name: Application4G_ henBGrpMessageQueueOverloadMinimumThreshold (12958) Type: equipmentAlarm Package: femto.Application4G_ henBGrpMessageQueueOverloadMinimumThreshold Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the minimum message queue overload threshold has been exceeded for the HeNBGroup processes.		
Remedial action: This alarm is cleared when either the measured HenBGrp process main message queue usage falls below the minimum threshold or rises above the maximum threshold.. If the alarm persists for a long duration and not cleared on its own, terminate some calls and check whether message queue utilization comes down and the alarm is cleared.If message queue utilization does not come down and alarm is still present, de-register the Small Cells in a phased manner and check whether queue utilization comes down.For further assistance please contact NOKIA customer support.		

Table 28-29 Application4G_henbIdClash

Alarm	Attributes	Applicable major release
Name: Application4G_henbIdClash (5698) Type: operationalViolation Package: femto.Application4G_henbIdClash Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: callEstablishmentError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW has detected that another HENB tries to register with a henbId already used by another HeNB.		
Remedial action: Re-configure the Small Cell with a different ID.Re-register the Small Cell.		

Table 28-30 Application4G_henbIntegrityViolation

Alarm	Attributes	Applicable major release
Name: Application4G_henbIntegrityViolation (5699) Type: securityServiceOrMechanismViolation Package: femto.Application4G_henbIntegrityViolation Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authenticationFailure	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW has detected a mismatch between the parameters received from the HeNB SETUP Request and the provisioned HeNB parameters. At least one of the following parameters might have been manipulated:- HeNB-Id,- TAC- Access mode		
Remedial action: Verify, that the HeNB-Id, TAC and access mode of the registered Small Cell is same as present in BSR DATA XML file.Re-register this Small Cell.		

Table 28-31 Application4G_heNbOutOfService

Alarm	Attributes	Applicable major release
Name: Application4G_heNbOutOfService (5697) Type: equipmentAlarm Package: femto.Application4G_heNbOutOfService Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is triggered for HeNBs which have not registered with the SCGW during either the HenbRegisterAfterFailure-Timer period or the HenbRegisterAfterInitTimer period and which have the Application4G::enableServiceMonitoringattribute set to True.		
Remedial action: The alarm is cleared by the Gateway whenApplication4G::enableServiceMonitoring attribute is disabled orthe failed Small Cell tries to reregister.		

Table 28-32 Application4G_invalidHeNBS1SetupMessage

Alarm	Attributes	Applicable major release
Name: Application4G_invalidHeNBS1SetupMessage (5700) Type: communicationsAlarm Package: femto.Application4G_ invalidHeNBS1SetupMessage Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW receives S1 SETUP message with an invalid HeNBId.		
Remedial action: Check whether any invalid IE is sent as part of Small Cell registration request.Check Fatal/Error logs in Log_FMG.log file with respect to decoding of Small Cell registration request.Use the above information to isolate the issue at Small Cell or BSR Gateway end.		

Table 28-33 Application4G_invalidS1flexConfiguration

Alarm	Attributes	Applicable major release
Name: Application4G_invalidS1flexConfiguration (5701) Type: processingErrorAlarm Package: femto.Application4G_ invalidS1flexConfiguration Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is generated if the TAI in the INITIAL UE MESSAGE does not match the PLMN ID and TAC for an MME Region.		
Remedial action: Check the provisioned S1 Flex configuration function.		

Table 28-34 Application4G_massHeNbOutOfService

Alarm	Attributes	Applicable major release
Name: Application4G_massHeNbOutOfService (5702) Type: equipmentAlarm Package: femto.Application4G_ massHeNbOutOfService Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is triggered when the number of active bsrOutOfService alarms reaches the threshold defined by the Application4G:: maxNumHenbServiceAlarms attribute		
Remedial action: The alarm is automatically detected and cleared by the Gateway, when the total number of failed Small Cells drops below the Application4G:: maxNumHenbServiceAlarms value.		

Table 28-35 Application4G_massNBHeNbOutOfService

Alarm	Attributes	Applicable major release
Name: Application4G_massNBHeNbOutOfService (12737) Type: equipmentAlarm Package: femto.Application4G_ massNBHeNbOutOfService Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is triggered when the number of active nbHeNbOutOfService alarms reaches the threshold defined by the Application4G:: maxNumHenbServiceAlarms attribute		
Remedial action: The alarm is automatically detected and cleared by the Gateway, when the total number of failed NB-IOT Small Cells drops below the Application4G:: maxNumHenbServiceAlarms value.		

Table 28-36 Application4G_nbHeNbOutOfService

Alarm	Attributes	Applicable major release
Name: Application4G_nbHeNbOutOfService (12738) Type: equipmentAlarm Package: femto.Application4G_nbHeNbOutOfService Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is triggered for NB-IOT HeNBs which have not registered with the SCGW during either the HenbRegisterAfter-FailureTimer period or the HenbRegisterAfterInitTimer period and which have the Application4G::enableServiceMonitoring attribute set to True.		
Remedial action: The alarm is cleared by the Gateway whenApplication4G::enableServiceMonitoring attribute is disabled orthe failed NB-IOT Small Cell tries to reregister.		

Table 28-37 Application4G_newHeNBS1SetupRejectedDueToOverload

Alarm	Attributes	Applicable major release
Name: Application4G_ newHeNBS1SetupRejectedDueToOverload (5703) Type: qualityOfServiceAlarm Package: femto.Application4G_ newHeNBS1SetupRejectedDueToOverload Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when SCGW rejects new HeNB SETUP request due to overload		
Remedial action: Check the loading on the FGW.FGW automatically drops new S1SetupRequest and InitialUE messages from HeNBs, Paging messages from MME sheds signaling messages load and after 30-60 seconds the alarm is cleared automatically by FGW.This fault is automatically cleared by the clear alarmAPPLICATION4G_ NEWHENBS1SETUPREJECTEDDUETOOVERLOADCLEARANCE.If the alarm is not cleared automatically by FGW after 60 seconds, then contact Nokia customer support.		

Table 28-38 Application4G_provisionedWBHeNBsThresholdExceeded

Alarm	Attributes	Applicable major release
Name: Application4G_ provisionedWBHeNBsThresholdExceeded (12959) Type: equipmentAlarm Package: femto.Application4G_ provisionedWBHeNBsThresholdExceeded Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is triggered when the number of provisioned WB HeNBs exceeds HeNBGW provisioned threshold limit(via Application4G::maxSupportedHeNBs attribute).		
Remedial action: Check if more than maxSupportedHeNBs (FGW threshold limit) WB entries are being sent in the HeNB data file to FGW from the OAM system. If yes take steps to limit the provisioning to threshold (currently 65535) for WB HeNBs. The operator must do a manual clearance for the alarm.		

Table 28-39 Application4G_s1pagingCapacityThresholdExceeded

Alarm	Attributes	Applicable major release
Name: Application4G_ s1pagingCapacityThresholdExceeded (12960) Type: equipmentAlarm Package: femto.Application4G_ s1pagingCapacityThresholdExceeded Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is triggered when the number of S1AP Paging received by the HeNBGW from MME exceeded the threshold HeNBGW limit.		
Remedial action: Check if more no of S1 Paging requests are received from MME than provisioned limit in parameter Applocation4G:: maxSupportedS1Paging.Check if Paging retries are happening from the MME and investigate the cause if there is a sudden or gradual incease during last few intervals. The operator must do a manual clearance for the alarm.For further assistance please contact Nokia Support.		

Table 28-40 Application4G_spareAlarmApplication4G1

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G1 (12394) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G1 Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-41 Application4G_spareAlarmApplication4G2

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G2 (12395) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G2 Raised on class: femto.Application4G	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-42 Application4G_spareAlarmApplication4G3

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G3 (12396) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G3 Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-43 Application4G_spareAlarmApplication4G4

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G4 (12961) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G4 Raised on class: femto.Application4G	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm 4		

Table 28-44 Application4G_spareAlarmApplication4G5

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G5 (12962) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G5 Raised on class: femto.Application4G	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm 5		

Table 28-45 Application4G_spareAlarmApplication4G6

Alarm	Attributes	Applicable major release
Name: Application4G_spareAlarmApplication4G6 (12963) Type: equipmentAlarm Package: femto.Application4G_ spareAlarmApplication4G6 Raised on class: femto.Application4G	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm 6		

Table 28-46 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator1

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator1 (12973) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator1 Raised on class: femto.ApplicationX2Aggregator	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-47 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator2

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator2 (12974) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator2 Raised on class: femto.ApplicationX2Aggregator	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-48 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator3

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator3 (12975) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator3 Raised on class: femto.ApplicationX2Aggregator	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-49 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator4

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator4 (12976) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator4 Raised on class: femto.ApplicationX2Aggregator	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm 4		

Table 28-50 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator5

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator5 (12977) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator5 Raised on class: femto.ApplicationX2Aggregator	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm 5		

Table 28-51 ApplicationX2Aggregator_spareAlarmApplicationX2Aggregator6

Alarm	Attributes	Applicable major release
Name: ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator6 (12978) Type: equipmentAlarm Package: femto.ApplicationX2Aggregator_ spareAlarmApplicationX2Aggregator6 Raised on class: femto.ApplicationX2Aggregator	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm 6		

Table 28-52 AtcaAlarmCard_e1InfraAlarm

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_e1InfraAlarm (5704) Type: communicationsAlarm Package: femto.AtcaAlarmCard_e1InfraAlarm Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmInterface	Release: • 4.0.0
Description: This Alarm is raised when there is a failure and the infrastructure alarms :E1_A, E1_B, E1_C, E1_D get raised.		
Remedial action: See the nodal documentation for more information.		

Table 28-53 AtcaAlarmCard_e2InfraAlarm

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_e2InfraAlarm (5705) Type: communicationsAlarm Package: femto.AtcaAlarmCard_e2InfraAlarm Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmInterface	Release: • 4.0.0
Description: This Alarm is raised when there is a failure and the infrastructure alarms : E2_A, E2_B, E2_C, E2_D get raised.		
Remedial action: See the nodal documentation for more information.		

Table 28-54 AtcaAlarmCard_e3InfraAlarm

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_e3InfraAlarm (5706) Type: communicationsAlarm Package: femto.AtcaAlarmCard_e3InfraAlarm Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmInterface	Release: • 4.0.0
Description: This Alarm is raised when there is a failure and the infrastructure alarms : E3_A, E3_B, E3_C, E3_D get raised.		

Table 28-54 AtcaAlarmCard_e3InfraAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: See the nodal documentation for more information.		

Table 28-55 AtcaAlarmCard_e4InfraAlram

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_e4InfraAlram (5707) Type: communicationsAlarm Package: femto.AtcaAlarmCard_e4InfraAlram Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteAlarmInterface	Release: • 4.0.0
Description: This Alarm is raised when there is a failure and the infrastructure alarms : E4_A, E4_B, E4_C, E4_D get raised.		
Remedial action: See the nodal documentation for more information.		

Table 28-56 AtcaAlarmCard_pdu

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_pdu (5708) Type: equipmentAlarm Package: femto.AtcaAlarmCard_pdu Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when there is failure in the PDU presence.		
Remedial action: See the nodal documentation for more information.		

Table 28-57 AtcaAlarmCard_pduBreakerPwr

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_pduBreakerPwr (5709) Type: environmentalAlarm Package: femto.AtcaAlarmCard_pduBreakerPwr Raised on class: femto.SCATCAAlarmCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when there is failure in AT1 PDU Breaker A, AT1 PDU Breaker B.		
Remedial action: See the nodal documentation for more information.		

Table 28-58 AtcaAlarmCard_pduFeedPwr

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_pduFeedPwr (5710) Type: environmentalAlarm Package: femto.AtcaAlarmCard_pduFeedPwr Raised on class: femto.SCATCAAlarmCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when there is failure in the AT1 PDU Feed A, AT1 PDU Feed B.		
Remedial action: See the nodal documentation for more information.		

Table 28-59 AtcaAlarmCard_powerFailure

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_powerFailure (5711) Type: environmentalAlarm Package: femto.AtcaAlarmCard_powerFailure Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when the Loop Voltage failure, VoltageFailure48V_A and VoltageFailure48V_B. happens		
Remedial action: See the nodal documentation for more information.		

Table 28-60 AtcaAlarmCard_telcoAlarmInput

Alarm	Attributes	Applicable major release
Name: AtcaAlarmCard_telcoAlarmInput (5712) Type: equipmentAlarm Package: femto.AtcaAlarmCard_telcoAlarmInput Raised on class: femto.SCATCAAlarmCard	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the System manager does the minor Reset, major Reset and Alarm cutoff.		
Remedial action: See the nodal documentation for more information.		

Table 28-61 AtcaCardTemperatureLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardTemperatureLowerThresholdAlarm (3710) Type: equipmentAlarm Package: equipment. AtcaCardTemperatureLowerThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardTemperatureLow	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the ATCA card temperature has decreased below any of the lower thresholds.		

Table 28-61 AtcaCardTemperatureLowerThresholdAlarm (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Temperature Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Informational - no corrective action required.		

Table 28-62 AtcaCardTemperatureUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardTemperatureUpperThresholdAlarm (3711) Type: equipmentAlarm Package: equipment. AtcaCardTemperatureUpperThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardTemperatureHigh	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the ATCA card temperature has increased beyond any of the upper thresholds.		
Raising condition: ('Temperature Threshold State' EQUAL 'Upper Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor the blade. If the condition persists, replace the blade. If the condition applies to more than one blade, verify the performance of the site cooling system.		

Table 28-63 AtcaCardVoltageLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardVoltageLowerThresholdAlarm (3712) Type: equipmentAlarm Package: equipment. AtcaCardVoltageLowerThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardVoltageLow	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the ATCA card voltage level has decreased below any of the lower thresholds.		
Raising condition: ('Voltage Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the blade is in the active state, it should be replaced.		

Table 28-64 AtcaCardVoltageUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardVoltageUpperThresholdAlarm (3713) Type: equipmentAlarm Package: equipment. AtcaCardVoltageUpperThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardVoltageHigh	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the ATCA card voltage level has increased beyond any of the upper thresholds.		
Raising condition: ('Voltage Threshold State' EQUAL 'Upper Critical')		
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the blade is in the active state, it should be replaced.		

Table 28-65 AtcaFanTray_fanAgingDown1

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown1 (5713) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown1 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging1		
Remedial action: See the nodal documentation for more information.		

Table 28-66 AtcaFanTray_fanAgingDown2

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown2 (5714) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown2 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging2		
Remedial action: See the nodal documentation for more information.		

Table 28-67 AtcaFanTray_fanAgingDown3

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown3 (5715) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown3 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging3		
Remedial action: See the nodal documentation for more information.		

Table 28-68 AtcaFanTray_fanAgingDown4

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown4 (5716) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown4 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging4		
Remedial action: See the nodal documentation for more information.		

Table 28-69 AtcaFanTray_fanAgingDown5

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown5 (5717) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown5 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging5		
Remedial action: See the nodal documentation for more information.		

Table 28-70 AtcaFanTray_fanAgingDown6

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingDown6 (5718) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingDown6 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Down fan tray reaches the Aging6		
Remedial action: See the nodal documentation for more information.		

Table 28-71 AtcaFanTray_fanAgingRear1

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear1 (5719) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear1 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging1		
Remedial action: See the nodal documentation for more information.		

Table 28-72 AtcaFanTray_fanAgingRear2

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear2 (5720) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear2 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging2		
Remedial action: See the nodal documentation for more information.		

Table 28-73 AtcaFanTray_fanAgingRear3

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear3 (5721) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear3 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging3		
Remedial action: See the nodal documentation for more information.		

Table 28-74 AtcaFanTray_fanAgingRear4

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear4 (5722) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear4 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging4		
Remedial action: See the nodal documentation for more information.		

Table 28-75 AtcaFanTray_fanAgingRear5

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear5 (5723) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear5 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging5		
Remedial action: See the nodal documentation for more information.		

Table 28-76 AtcaFanTray_fanAgingRear6

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingRear6 (5724) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingRear6 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Rear fan tray reaches the Aging6		
Remedial action: See the nodal documentation for more information.		

Table 28-77 AtcaFanTray_fanAgingUp1

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp1 (5725) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp1 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging1		
Remedial action: See the nodal documentation for more information.		

Table 28-78 AtcaFanTray_fanAgingUp2

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp2 (5726) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp2 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging2		
Remedial action: See the nodal documentation for more information.		

Table 28-79 AtcaFanTray_fanAgingUp3

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp3 (5727) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp3 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging3		
Remedial action: See the nodal documentation for more information.		

Table 28-80 AtcaFanTray_fanAgingUp4

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp4 (5728) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp4 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging4		
Remedial action: See the nodal documentation for more information.		

Table 28-81 AtcaFanTray_fanAgingUp5

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp5 (5729) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp5 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging5		
Remedial action: See the nodal documentation for more information.		

Table 28-82 AtcaFanTray_fanAgingUp6

Alarm	Attributes	Applicable major release
Name: AtcaFanTray_fanAgingUp6 (5730) Type: equipmentAlarm Package: femto.AtcaFanTray_fanAgingUp6 Raised on class: femto.SCATCAFanTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitProblem	Release: • 4.0.0
Description: This Alarm is raised when the Upper fan tray reaches the Aging6		
Remedial action: See the nodal documentation for more information.		

Table 28-83 AtcaShelfManager_boardFilterAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_boardFilterAbsence (5731) Type: equipmentAlarm Package: femto.AtcaShelfManager_ boardFilterAbsence Raised on class: femto.SCATCAShelfManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0
Description: This Alarm is raised when the Board filter or the Front side filter or grid is not present.		
Remedial action: See the nodal documentation for more information.		

Table 28-84 AtcaShelfManager_cpldSensor

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_cpldSensor (5732) Type: equipmentAlarm Package: femto.AtcaShelfManager_cpldSensor Raised on class: femto.SCATCAShelfManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when there is change in the shelf manager redundancy status.		
Remedial action: See the nodal documentation for more information.		

Table 28-85 AtcaShelfManager_fanTrayLowAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_fanTrayLowAbsence (5733) Type: equipmentAlarm Package: femto.AtcaShelfManager_ fanTrayLowAbsence Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0
Description: This Alarm is raised when the Lower fan tray is not present.		
Remedial action: See the nodal documentation for more information.		

Table 28-86 AtcaShelfManager_fanTrayRearAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_fanTrayRearAbsence (5734) Type: equipmentAlarm Package: femto.AtcaShelfManager_ fanTrayRearAbsence Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0

Table 28-86 AtcaShelfManager_fanTrayRearAbsence (continued)

Alarm	Attributes	Applicable major release
Description: This Alarm is raised when the Rear fan tray is not present.		
Remedial action: See the nodal documentation for more information.		

Table 28-87 AtcaShelfManager_fanTraysFRUcriticalFailure

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_fanTraysFRUcriticalFailure (5736) Type: equipmentAlarm Package: femto.AtcaShelfManager_ fanTraysFRUcriticalFailure Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure occurs in the Fan Trays FRUs.		
Remedial action: See the nodal documentation for more information.		

Table 28-88 AtcaShelfManager_fanTrayUpAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_fanTrayUpAbsence (5735) Type: equipmentAlarm Package: femto.AtcaShelfManager_ fanTrayUpAbsence Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0
Description: This Alarm is raised when the Up fan tray is not present.		
Remedial action: See the nodal documentation for more information.		

Table 28-89 AtcaShelfManager_i2cLocalBus

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_i2cLocalBus (5737) Type: equipmentAlarm Package: femto.AtcaShelfManager_i2cLocalBus Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to the I2C Local Bus.		
Remedial action: See the nodal documentation for more information.		

Table 28-90 AtcaShelfManager_i2cMasterResourceHighLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_ i2cMasterResourceHighLimit (5738) Type: equipmentAlarm Package: femto.AtcaShelfManager_ i2cMasterResourceHighLimit Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the I2C Master Resource reaches the critical limit.		
Remedial action: See the nodal documentation for more information.		

Table 28-91 AtcaShelfManager_i2cMasterResourceMidLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_i2cMasterResourceMidLimit (5739) Type: equipmentAlarm Package: femto.AtcaShelfManager_ i2cMasterResourceMidLimit Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the I2C of the Master Resource reaches the major limit		
Remedial action: See the nodal documentation for more information.		

Table 28-92 AtcaShelfManager_ipmbLinkDown

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_ipmbLinkDown (5740) Type: equipmentAlarm Package: femto.AtcaShelfManager_ipmbLinkDown Raised on class: femto.SCATCAShelfManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to the IPMB-0 link		
Remedial action: See the nodal documentation for more information.		

Table 28-93 AtcaShelfManager_lm75TempDownHighLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_lm75TempDownHighLimit (5741) Type: environmentalAlarm Package: femto.AtcaShelfManager_ lm75TempDownHighLimit Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lowTemperature	Release: • 4.0.0
Description: This Alarm is raised when the temperature of the bottom of the NBSHMC board reaches the lower critical limit.		
Remedial action: See the nodal documentation for more information.		

Table 28-94 AtcaShelfManager_lm75TempDownMidLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_lm75TempDownMidLimit (5742) Type: environmentalAlarm Package: femto.AtcaShelfManager_ lm75TempDownMidLimit Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lowTemperatureMidLimit	Release: • 4.0.0
Description: This Alarm is raised when the temperature of the bottom of the NBSHMC board reaches the lower major limit.		
Remedial action: See the nodal documentation for more information.		

Table 28-95 AtcaShelfManager_lm75TempUpHighLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_lm75TempUpHighLimit (5743) Type: environmentalAlarm Package: femto.AtcaShelfManager_ lm75TempUpHighLimit Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: highTemperature	Release: • 4.0.0
Description: This Alarm is raised when the temperature of the top of the NBSHMC board reaches the upper critical limit.		
Remedial action: See the nodal documentation for more information.		

Table 28-96 AtcaShelfManager_lm75TempUpMidLimit

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_lm75TempUpMidLimit (5744) Type: environmentalAlarm Package: femto.AtcaShelfManager_ lm75TempUpMidLimit Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: highTemperature	Release: • 4.0.0
Description: This Alarm is raised when the temperature of the top of the NBSHMC board reaches the upper major limit.		
Remedial action: See the nodal documentation for more information.		

Table 28-97 AtcaShelfManager_pwrRedDegraded

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_pwrRedDegraded (5745) Type: equipmentAlarm Package: femto.AtcaShelfManager_pwrRedDegraded Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: Power supple redundancy degraded assert. Redundancy still exists, but at a less than full level. For example, a system has four fans, and can tolerate the failure of two of them, and presently one has failed		
Remedial action: See the nodal documentation for more information.		

Table 28-98 AtcaShelfManager_pwrRedLost

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_pwrRedLost (5746) Type: equipmentAlarm Package: femto.AtcaShelfManager_pwrRedLost Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Power supply redundancy lost or Entered any non-redundant state, including Non-redundant: Insufficient Resources		
Remedial action: See the nodal documentation for more information.		

Table 28-99 AtcaShelfManager_pwrRedRegained

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_pwrRedRegained (5747) Type: equipmentAlarm Package: femto.AtcaShelfManager_pwrRedRegained Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0

Table 28-99 AtcaShelfManager_pwrRedRegained (continued)

Alarm	Attributes	Applicable major release
Description: This Alarm is raised when the full power supply redundancy has been regained		
Remedial action: See the nodal documentation for more information.		

Table 28-100 AtcaShelfManager_rebootReason

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_rebootReason (5748) Type: equipmentAlarm Package: femto.AtcaShelfManager_rebootReason Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Shelf Manager has been Rebooted		
Remedial action: See the nodal documentation for more information.		

Table 28-101 AtcaShelfManager_rtmFilterAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_rtmFilterAbsence (5749) Type: equipmentAlarm Package: femto.AtcaShelfManager_rtmFilterAbsence Raised on class: femto.SCATCAShelfManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0
Description: This Alarm is raised when the RTM filter or the Back side filter or grid is not present.		
Remedial action: See the nodal documentation for more information.		

Table 28-102 AtcaShelfManager_shelfFRUcriticalFailure

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_shelfFRUcriticalFailure (5750) Type: equipmentAlarm Package: femto.AtcaShelfManager_ shelfFRUcriticalFailure Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when critical failure happens to the Shelf FRUs in EEPROMs.		
Remedial action: See the nodal documentation for more information.		

Table 28-103 AtcaShelfManager_shelfFRUminorFailure

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_shelfFRUminorFailure (5751) Type: equipmentAlarm Package: femto.AtcaShelfManager_ shelfFRUminorFailure Raised on class: femto.SCATCAShelfManager	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when minor failure happens to the Shelf FRUs in EEPROMs.		
Remedial action: See the nodal documentation for more information.		

Table 28-104 AtcaShelfManager_shelfManagerConnectionFailure

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_ shelfManagerConnectionFailure (5752) Type: communicationsAlarm Package: femto.AtcaShelfManager_ shelfManagerConnectionFailure Raised on class: femto.SCATCAShelfManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 4.0.0
Description: This Alarm is raised when the Shelf Oam is unable to communicate with shelf manager		
Remedial action: See the nodal documentation for more information.		

Table 28-105 AtcaShelfManager_shelfManagerInNonRedundantState

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_ shelfManagerInNonRedundantState (5753) Type: communicationsAlarm Package: femto.AtcaShelfManager_ shelfManagerInNonRedundantState Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 4.0.0
Description: This Alarm is raised when the Peer Shelf Manager is not available		
Remedial action: See the nodal documentation for more information.		

Table 28-106 AtcaShelfManager_shelfManagerUnAvailable

Alarm	Attributes	Applicable major release
Name: AtcaShelfManager_shelfManagerUnAvailable (5754) Type: equipmentAlarm Package: femto.AtcaShelfManager_ shelfManagerUnAvailable Raised on class: femto.SCATCAShelfManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Shelf Manager Card is not available		
Remedial action: See the nodal documentation for more information.		

Table 28-107 AtcaShelf_alarmCardAbsence

Alarm	Attributes	Applicable major release
Name: AtcaShelf_alarmCardAbsence (5755) Type: equipmentAlarm Package: femto.AtcaShelf_alarmCardAbsence Raised on class: femto.SCATCAShelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: probCauseUnknown	Release: • 4.0.0
Description: This Alarm is raised when there is failure in the Alarm card presence.		
Remedial action: See the nodal documentation for more information.		

Table 28-108 AtcaSwitchBaseEthernetIntf_malbanBaseEthernetPortFailure

Alarm	Attributes	Applicable major release
Name: AtcaSwitchBaseEthernetIntf_ malbanBaseEthernetPortFailure (5756) Type: equipmentAlarm Package: femto.AtcaSwitchBaseEthernetIntf_ malbanBaseEthernetPortFailure Raised on class: femto. SCATCASwitchBaseEthernetIntf	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Malban Card Base Ethernet port has failed		
Remedial action: See the nodal documentation for more information.		

Table 28-109 AtcaSwitchCPU_malban10CPUFailure

Alarm	Attributes	Applicable major release
Name: AtcaSwitchCPU_malban10CPUFailure (5757) Type: equipmentAlarm Package: femto.AtcaSwitchCPU_ malban10CPUFailure Raised on class: femto.SCATCASwitchCPU	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: processorProblem	Release: • 4.0.0
Description: This Alarm is raised when software critical error occurs on the payload. Usually followed by a board reboot or reset. It is asserted upon fault detection by the payload software and de-asserted on startup.		
Remedial action: See the nodal documentation for more information.		

Table 28-110 AtcaSwitchFabricEthernetIntf_malbanFabricEthernetPortFailure

Alarm	Attributes	Applicable major release
Name: AtcaSwitchFabricEthernetIntf_ malbanFabricEthernetPortFailure (5758) Type: equipmentAlarm Package: femto.AtcaSwitchFabricEthernetIntf_ malbanFabricEthernetPortFailure Raised on class: femto. SCATCASwitchFabricEthernetIntf	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Malban Card Fabric Ethernet port has failed		
Remedial action: See the nodal documentation for more information.		

Table 28-111 AtcaSwitchSlot_malbanConnectionFailure

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_malbanConnectionFailure (5759) Type: communicationsAlarm Package: femto.AtcaSwitchSlot_ malbanConnectionFailure Raised on class: femto.SCATCASwitchSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 4.0.0
Description: This Alarm is raised when the Shelf Oam is unable to communicate with Malban		
Remedial action: See the nodal documentation for more information.		

Table 28-112 AtcaSwitchSlot_malbanInNonRedundantState

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_malbanInNonRedundantState (5760) Type: communicationsAlarm Package: femto.AtcaSwitchSlot_malbanInNonRedundantState Raised on class: femto.SCATCASwitchSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 4.0.0
Description: This Alarm is raised when the Peer Malban is not available		
Remedial action: See the nodal documentation for more information.		

Table 28-113 AtcaSwitchSlot_malbanIpmbLinkDown

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_malbanIpmbLinkDown (5761) Type: equipmentAlarm Package: femto.AtcaSwitchSlot_malbanIpmbLinkDown Raised on class: femto.SCATCASwitchSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to the IPMB-0 link		
Remedial action: See the nodal documentation for more information.		

Table 28-114 AtcaSwitchSlot_malbanUnAvailable

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_malbanUnAvailable (5762) Type: equipmentAlarm Package: femto.AtcaSwitchSlot_malbanUnAvailable Raised on class: femto.SCATCASwitchSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when the Malban Card is not available		
Remedial action: See the nodal documentation for more information.		

Table 28-115 AtcaSwitchSlot_malbanVlanCreationFailure

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_malbanVlanCreationFailure (5763) Type: communicationsAlarm Package: femto.AtcaSwitchSlot_malbanVlanCreationFailure Raised on class: femto.SCATCASwitchSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 4.0.0

Table 28-115 AtcaSwitchSlot_malbanVlanCreationFailure (continued)

Alarm	Attributes	Applicable major release
Description: This Alarm is raised when the vlan creation failed in Malban		
Remedial action: See the nodal documentation for more information.		

Table 28-116 AtcaSwitchSlot_ncpuFatalError

Alarm	Attributes	Applicable major release
Name: AtcaSwitchSlot_ncpuFatalError (5764) Type: equipmentAlarm Package: femto.AtcaSwitchSlot_ncpuFatalError Raised on class: femto.SCATCASwitchSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when a software critical error occurs on the payload.		
Remedial action: See the nodal documentation for more information.		

Table 28-117 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 28-118 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-118 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 28-119 BladeHardware_alarm48VaAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_alarm48VaAssert (5861) Type: equipmentAlarm Package: femto.BladeHardware_alarm48VaAssert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Alarm 48Va assert		
Remedial action: Check the power supply of the ATCA chassis.		

Table 28-120 BladeHardware_alarm48VaDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_alarm48VaDeassert (5862) Type: equipmentAlarm Package: femto.BladeHardware_alarm48VaDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Alarm 48Va deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-121 BladeHardware_alarm48VbAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_alarm48VbAssert (5863) Type: equipmentAlarm Package: femto.BladeHardware_alarm48VbAssert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Alarm 48Vb assert		
Remedial action: Clear the alarms manually from the OAM system after replacing the blade hardware.		

Table 28-122 BladeHardware_alarm48VbDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_alarm48VbDeassert (5864) Type: equipmentAlarm Package: femto.BladeHardware_alarm48VbDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Alarm 48Vb deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-123 BladeHardware_bonoCardDeletionEvent

Alarm	Attributes	Applicable major release
Name: BladeHardware_bonoCardDeletionEvent (12969) Type: equipmentAlarm Package: femto.BladeHardware_ bonoCardDeletionEvent Raised on class: femto.BladeHardware	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: This alarm is generated when a bono card is pulled out or removed from either active or standby card slot of FGW in an ATCA shelf.		
Remedial action: The operator must do a manual clearance for the alarm.For further assistance, contact Nokia customer support.		

Table 28-124 BladeHardware_bonoCardInsertionEvent

Alarm	Attributes	Applicable major release
Name: BladeHardware_bonoCardInsertionEvent (12970) Type: equipmentAlarm Package: femto.BladeHardware_ bonoCardInsertionEvent Raised on class: femto.BladeHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: This alarm is generated when a bono card is inserted in either active or standby card slot of FGW in an ATCA shelf.		
Remedial action: The operator must do a manual clearance.		

Table 28-125 BladeHardware_bootOkAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_bootOkAssert (5865) Type: equipmentAlarm Package: femto.BladeHardware_bootOkAssert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Boot OK assert		
Remedial action: The operator must do a manual clearance.		

Table 28-126 BladeHardware_bootOkDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_bootOkDeassert (5866) Type: equipmentAlarm Package: femto.BladeHardware_bootOkDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Boot OK deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-127 BladeHardware_ipmbPhysicalAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ipmbPhysicalAssert (5867) Type: equipmentAlarm Package: femto.BladeHardware_ipmbPhysicalAssert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: IPMB physical assert		
Remedial action: Check the IPMB link sensor associated with the blade hardware.Perform switch over if the error appears at shelf manager level.Replace the blade hardware if the issue still continues.		

Table 28-128 BladeHardware_ipmbPhysicalDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ipmbPhysicalDeassert (5868) Type: equipmentAlarm Package: femto.BladeHardware_ipmbPhysicalDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: IPMB physical deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-129 BladeHardware_lm75localTempCriticalAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_lm75localTempCriticalAssert (5871) Type: equipmentAlarm Package: femto.BladeHardware_lm75localTempCriticalAssert Raised on class: femto.BladeHardware	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature critical assert		
Remedial action: Check BONO card temperature and cooling.For further assistance, contact Nokia customer support.		

Table 28-130 BladeHardware_lm75localTempCriticalAssLMert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ lm75localTempCriticalAssLMert (5870) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempCriticalAssLMert Raised on class: femto.BladeHardware	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: LM 75 local temperature critical assert		
Remedial action: The operator must do a manual clearance.		

Table 28-131 BladeHardware_lm75localTempCriticalDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ lm75localTempCriticalDeassert (5873) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempCriticalDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature critical deassert		
Remedial action: No action needed.Informational alarm indicating Bono card temperature has recovered within the range.		

Table 28-132 BladeHardware_lm75localTempCriticalDeassLMert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ lm75localTempCriticalDeassLMert (5872) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempCriticalDeassLMert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: LM 75 local temperature critical deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-133 BladeHardware_lm75LocalTempMajorAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_lm75LocalTempMajorAssert (5869) Type: equipmentAlarm Package: femto.BladeHardware_ lm75LocalTempMajorAssert Raised on class: femto.BladeHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature major assert		
Remedial action: Clear the alarms manually from the OAM system after replacing the blade hardware.		

Table 28-134 BladeHardware_lm75localTempMajorDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_lm75localTempMajorDeassert (5874) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempMajorDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature major deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-135 BladeHardware_lm75localTempMinorAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_lm75localTempMinorAssert (5875) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempMinorAssert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature minor assert		
Remedial action: The operator must do a manual clearance.		

Table 28-136 BladeHardware_lm75localTempMinorDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_lm75localTempMinorDeassert (5876) Type: equipmentAlarm Package: femto.BladeHardware_ lm75localTempMinorDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LM 75 local temperature minor deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-137 BladeHardware_ncpuFatalErrAssert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ncpuFatalErrAssert (5877) Type: equipmentAlarm Package: femto.BladeHardware_ncpuFatalErrAssert Raised on class: femto.BladeHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: NCPU fatal assert		
Remedial action: The operator must do a manual clearance.		

Table 28-138 BladeHardware_ncpuFatalErrDeassert

Alarm	Attributes	Applicable major release
Name: BladeHardware_ncpuFatalErrDeassert (5878) Type: equipmentAlarm Package: femto.BladeHardware_ ncpuFatalErrDeassert Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: NCPU fatal deassert		
Remedial action: The operator must do a manual clearance.		

Table 28-139 BladeHardware_powerConsumptionMinor

Alarm	Attributes	Applicable major release
Name: BladeHardware_powerConsumptionMinor (5879) Type: equipmentAlarm Package: femto.BladeHardware_ powerConsumptionMinor Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Power consumption minor		
Remedial action: Check power connectivity to blade.		

Table 28-140 BladeHardware_spareAlarmBHADAC1

Alarm	Attributes	Applicable major release
Name: BladeHardware_spareAlarmBHADAC1 (8472) Type: equipmentAlarm Package: femto.BladeHardware_ spareAlarmBHADAC1 Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-141 BladeHardware_spareAlarmBHADAC2

Alarm	Attributes	Applicable major release
Name: BladeHardware_spareAlarmBHADAC2 (8473) Type: equipmentAlarm Package: femto.BladeHardware_ spareAlarmBHADAC2 Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-142 BladeHardware_spareAlarmBHADAC3

Alarm	Attributes	Applicable major release
Name: BladeHardware_spareAlarmBHADAC3 (8474) Type: equipmentAlarm Package: femto.BladeHardware_ spareAlarmBHADAC3 Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-143 BladeHardware_spareAlarmBHADAC4

Alarm	Attributes	Applicable major release
Name: BladeHardware_spareAlarmBHADAC4 (8475) Type: equipmentAlarm Package: femto.BladeHardware_ spareAlarmBHADAC4 Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm 4		

Table 28-144 BladeHardware_spareAlarmBHADAC5

Alarm	Attributes	Applicable major release
Name: BladeHardware_spareAlarmBHADAC5 (8476) Type: equipmentAlarm Package: femto.BladeHardware_ spareAlarmBHADAC5 Raised on class: femto.BladeHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm 5		

Table 28-145 BladeHardware_switchConnectionLost

Alarm	Attributes	Applicable major release
Name: BladeHardware_switchConnectionLost (5880) Type: equipmentAlarm Package: femto.BladeHardware_ switchConnectionLost Raised on class: femto.BladeHardware	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Switch connection lost		
Remedial action: The operator must do a manual clearance for this alarm.For further assistance, contact Nokia customer support.		

Table 28-146 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 28-147 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 28-147 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 28-148 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 28-149 BPG_noBpgMapping

Alarm	Attributes	Applicable major release
Name: BPG_noBpgMapping (5765) Type: processingErrorAlarm Package: femto.BPG_noBpgMapping Raised on class: femto.BPG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the BPG function receives a user plane packet which gets discarded due to there being no associated binding in the BPG mapping table.		
Remedial action: This alarm is generated when the BPG application receives a (user plane) voice packet, which gets discarded, due to there is no GTP-U packet between the Small Cell and BTG.Identify the Small Cell for which the alarm was raised in WMS with the patternBPG_NOBPGMAPPINGalarm raised for Small Cell.Initiate a voice call between the Small Cell and the core network. Verify that the connection is established between the Small Cell and BTG, through BTGConsole. Run the BTGConsole application and enter btg_get_bpg_table. A rule must be present for the corresponding Small Cell and core network.		

Table 28-150 BSG_aBSGUeRegTableFull

Alarm	Attributes	Applicable major release
Name: BSG_aBSGUeRegTableFull (5766) Type: equipmentAlarm Package: femto.BSG_aBSGUeRegTableFull Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the UE Registration Table has become full and existing entries have been discarded to make space for new entries		
Remedial action: Perform a UE de-registration to check whether the alarm is auto cleared.If Step 1 does not resolve the issue, de-register Small Cells and check whether alarm is auto cleared.The UE registration table is an internal BSR Gateway data structure, and the BSR Gateway auto clears the alarm when the count in the directory is below the maximum limit.		

Table 28-151 BSG_allocationOfStreamFail

Alarm	Attributes	Applicable major release
Name: BSG_allocationOfStreamFail (5767) Type: qualityOfServiceAlarm Package: femto.BSG_allocationOfStreamFail Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: congestion	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to allocate requested stream ID by BSR		
Remedial action: This alarm is cleared only if the streams are available for establishment of a call.The streams are freed by terminating the mobile originated calls.		

Table 28-152 BSG_bsgMessageQueueOverloadMaximumThreshold

Alarm	Attributes	Applicable major release
Name: BSG_ bsgMessageQueueOverloadMaximumThreshold (12964) Type: equipmentAlarm Package: femto.BSG_ bsgMessageQueueOverloadMaximumThreshold Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfMessageQueue	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the maximum message queue overload threshold has been exceeded for the BSG process.		
Remedial action: The FGW may initiate a failover to the available standby FGW if CPU or Memory maximum thresolds also get exceeded along with BSG message queue threshold. If significant detoriation in KPIs is seen perform forceful FGW switch-over manually.For further assistance please contact NOKIA customer support.		

Table 28-153 BSG_bsgMessageQueueOverloadMinimumThreshold

Alarm	Attributes	Applicable major release
Name: BSG_ bsgMessageQueueOverloadMinimumThreshold (12965) Type: equipmentAlarm Package: femto.BSG_ bsgMessageQueueOverloadMinimumThreshold Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is raised whenever the FGW has detected that the minimum message queue overload threshold has been exceeded for the BSG process.		
Remedial action: This alarm is cleared when either the measured BSG process SCTP message queue usage falls below the minimum threshold or rises above the maximum threshold. If the alarm persists for a long duration and not cleared on its own, terminate some calls and check whether message queue utilization comes down and the alarm is cleared.If message queue utilization does not come down and alarm is still present, de-register the Small Cells in a phased manner and check whether queue utilization comes down.For further assistance please contact NOKIA customer support.		

Table 28-154 BSG_bsgppPagingHighRateExceeded

Alarm	Attributes	Applicable major release
Name: BSG_bsgppPagingHighRateExceeded (5768) Type: processingErrorAlarm Package: femto.BSG_bsgppPagingHighRateExceeded Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the number of bsgpp Batch Paging messages processed per second has exceeded its High limit. Batch Paging is either greater than the configurable high CPU utilization or greater than the configurable High Batch Paging message rate. The number of Batch Paging messages sent shall be degraded to a rate within bounds.		
Remedial action: This alarm is cleared automatically from the OAM system when the number of batch paging messages processedper second is lower than the batch paging overload high value defined in the BSG, after sustain period configured in the BSG.		

Table 28-155 BSG_bsgppPagingLowRateExceeded

Alarm	Attributes	Applicable major release
Name: BSG_bsgppPagingLowRateExceeded (5769) Type: processingErrorAlarm Package: femto.BSG_bsgppPagingLowRateExceeded Raised on class: femto.BSG	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the number of bsgpp Batch Paging messages processed per second has exceeded its Low limit. Batch Paging is either greater than the configurable low CPU utilization or greater than the configurable Low Batch Paging message rate.		

Table 28-155 BSG_bsgppPagingLowRateExceeded (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is cleared automatically from the OAM system when the number of batch paging messages processedper second is lower than the batch paging overload low value defined in the BSG, after sustain period configured in the BSG.		

Table 28-156 BSG_bsrOutOfService

Alarm	Attributes	Applicable major release
Name: BSG_bsrOutOfService (5770) Type: equipmentAlarm Package: femto.BSG_bsrOutOfService Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is triggered for BSRs which have not registered with the SCGW during either the bsrRegisterAfterFailureTimer period or the bsrRegisterAfterInitTimer period and which have the BSR::enableServiceMonitoringattribute set to True.		
Remedial action: The alarm is automatically detected and cleared by the BSR Gateway when:BSR::enableServiceMonitoring attribute is disabled.The failed Small Cell tries to reregister.		

Table 28-157 BSG_cellBroadcastConflictingServiceArea

Alarm	Attributes	Applicable major release
Name: BSG_cellBroadcastConflictingServiceArea (5771) Type: processingErrorAlarm Package: femto.BSG_ cellBroadcastConflictingServiceArea Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm shall be raised when a Small Cell registers a Broadcast Service Area Identifier already in use by another Small Cell.		
Remedial action: Check the small cell's configuration to determine the cause of the incorrect Broadcast Service Area Identifier.		

Table 28-158 BSG_cellBroadcastInvalidServiceArea

Alarm	Attributes	Applicable major release
Name: BSG_cellBroadcastInvalidServiceArea (5772) Type: processingErrorAlarm Package: femto.BSG_cellBroadcastInvalidServiceArea Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-158 BSG_cellBroadcastInvalidServiceArea (continued)

Alarm	Attributes	Applicable major release
Description: This alarm shall be raised when a Small Cell attempts to register a Broadcast Service Area Identifier which does not correspond to the one provisioned for that Small Cell.		
Remedial action: Check the small cell's configuration to determine the cause of the incorrect Broadcast Service Area Identifier.		

Table 28-159 BSG_collapsingLAI

Alarm	Attributes	Applicable major release
Name: BSG_collapsingLAI (5773) Type: processingErrorAlarm Package: femto.BSG_collapsingLAI Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised when a SC requests the identity of a PSC/UARFCN that can only be matched to an entry from a different SC group, but with the same LAI		
Remedial action: Check LAI planning and consider changing LAI of one of the impacted SC groups.This alarm needs to be manually cleared from the OAM system.For further assistance contact Nokia customer support.		

Table 28-160 BSG_conflictingNeighboursDiscovered

Alarm	Attributes	Applicable major release
Name: BSG_conflictingNeighboursDiscovered (8464) Type: processingErrorAlarm Package: femto.BSG_ conflictingNeighboursDiscovered Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: An Access Point has reported neighbours with conflicting PSC setting		
Remedial action: Perform a self optimisaton of the BSRs identified in the additional information for this alarm at the next opportunity		

Table 28-161 BSG_differentLacRacSameGroup

Alarm	Attributes	Applicable major release
Name: BSG_differentLacRacSameGroup (5774) Type: processingErrorAlarm Package: femto.BSG_differentLacRacSameGroup Raised on class: femto.BSG	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when a Femto belonging to a Group has tried to register with a different Macro LAC RAC than other Femtos belonging to the same Group.		

Table 28-161 BSG_differentLacRacSameGroup (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is cleared automatically from the OAM system when the BSG accepts new registration requests from Small Cells having different group ids with the different macro LAC RAC values.		

Table 28-162 BSG_differentMacroLacRacDetected

Alarm	Attributes	Applicable major release
Name: BSG_differentMacroLacRacDetected (5775) Type: processingErrorAlarm Package: femto.BSG_differentMacroLacRacDetected Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when Femto registration contains a Macro LAC RAC that is not provisioned on the BSG..		
Remedial action: This alarm is cleared automatically from the OAM system when theBSG is configured with macro LAC RAC andaccepts new registration requests from the Small Cell.		

Table 28-163 BSG_droppingRANAPTraffic

Alarm	Attributes	Applicable major release
Name: BSG_droppingRANAPTraffic (5776) Type: qualityOfServiceAlarm Package: femto.BSG_droppingRANAPTraffic Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW drops RANAP traffic since SCGW CPU/Memory utilization has crossed maximum threshold		
Remedial action: The alarm is cleared when the BSR Gateway recovers from the overload condition by the clear alarm BSG_DROPPINGRANAPTRAFFICCLEARANCEThe %CPU column of top command can be used to check the CPU utilization.Enter the command free -m to check the memory utilization. Free memory specified should be high compared to the used memory available,for recovering to normal overload. The used buffer cache memory should be low. To drop the cache memory use the command echo 3 >/proc/sys/vm/drop_caches.Terminate some calls to check whether memory utilization comes down, clearing thealarm.If the memory utilization does not reduce and the alarm persists, de-register the Femtocells and check for reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforcedFemtocell de-registration, enforce a BSR Gateway switch-over by terminating the BSR Gateway application.If the problem persists, contact Nokia customer support.		

Table 28-164 BSG_failedIMSIRetrieval

Alarm	Attributes	Applicable major release
Name: BSG_failedIMSIRetrieval (5777) Type: equipmentAlarm Package: femto.BSG_failedIMSIRetrieval Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW is not able to retrieve the IMSI directory entries		
Remedial action: Check the directory bsg_get_imsi_directory to view the IMSI list.Clear the alarms manually from the OAM system if IMSIs are successfully retrieved.		

Table 28-165 BSG_failedToDecodeMSCSentMsg

Alarm	Attributes	Applicable major release
Name: BSG_failedToDecodeMSCSentMsg (5778) Type: communicationsAlarm Package: femto.BSG_failedToDecodeMSCSentMsg Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is triggered when SCGW fails to decode messages sent by 3G-MSC		
Remedial action: Check whether the following IEs are properly framed and sent by the MSC/SGSN: RAB Assignment Request CommonId Paging Reset Reset Acknowledge Reset Resource Reset Resource Acknowledge Relocation RequestCheck if any CS specific IEs (For example, relocation request) are sent for PS calls by the SGSN.This fault is cleared manually from the SCMS.If the problem persists, contact Nokia customer support.		

Table 28-166 BSG_failedToSendDataToBSR

Alarm	Attributes	Applicable major release
Name: BSG_failedToSendDataToBSR (5779) Type: communicationsAlarm Package: femto.BSG_failedToSendDataToBSR Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send data to BSR		
Remedial action: Check the connectivity between the Small Cell and BSR Gateway.Check whether the BSR Gateway sctp port (6005) towards Small Cell is open.Check for any errors with respect to sending the data towards Small Cell. This can be done by looking for LOG ERROR statements in LOG_FMG.log file under /opt/log/.Use the above mentioned information to isolate the issue at Small Cell or BSR Gateway.This alarm is cleared when data from the BSR Gateway reaches the Small Cell successfully.It is verified by executing successful IuCS/IuPS calls.For further assistance contact Nokia customer support.		

Table 28-167 BSG_failedToSendDataToMSC

Alarm	Attributes	Applicable major release
Name: BSG_failedToSendDataToMSC (5780) Type: communicationsAlarm Package: femto.BSG_failedToSendDataToMSC Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send data to 3G-MSC		
Remedial action: Reduce memory utilization in BSR Gateway, using the command free -m. Check if there is a reduction.Check whether memory overload alarm has been triggered.Terminate some calls to check if the memory utilization reduces, clearing the alarm.If there is no reduction in memory utilization, and the overload alarm still persists,then de-register the Femtocells. Now check for any reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforcedFemtocell de-registration. Enforce a BSR Gateway switchover by terminating the BSR Gateway applicationIf the problem persists, contact Nokia customer support.		

Table 28-168 BSG_groupNeighbourUsingAssignedPSC

Alarm	Attributes	Applicable major release
Name: BSG_groupNeighbourUsingAssignedPSC (8465) Type: processingErrorAlarm Package: femto.BSG_ groupNeighbourUsingAssignedPSC Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: An Access Point is reporting a detected Macro Cell which is using a PSC from the group's femtoPSCList but is not a member of this Femto Group		
Remedial action: Check the PSC configuration of the Macro Cells and the configuration of the PSC lists for this Femto Group		

Table 28-169 BSG_hnbIntegrityViolation

Alarm	Attributes	Applicable major release
Name: BSG_hnbIntegrityViolation (5781) Type: securityServiceOrMechanismViolation Package: femto.BSG_hnbIntegrityViolation Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authenticationFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when BSG has detected a mismatch between the registration parameters received from the BSR and the provisioned BSR parameters. At least one of the following parameters might have been manipulated:- Cell-Id,- HNB Identity		

Table 28-169 BSG_hnbIntegrityViolation (continued)

Alarm	Attributes	Applicable major release
Remedial action: This fault is raised when incoming Hnb Id or Cell Id parameter in the HNB Registration request is not available in theentries, present in the BSR DATA XML file /opt/bsrdata/OAM_BsrDataPersistentDB.txt. Check if the Hnb Id returned in the additional text is present in the /opt/bsrdata/OAM_BsrDataPersistentDB.txt file.If the received Hnb Id is present, then obtain the corresponding BSR ID from the/opt/bsrdata/OAM_BsrDataPersistentDB.txt and frame the Cell Id which is a combination of (MSB: BSG:bsr Id(16 bit) LSB: FGW:globalRNCIdRncId (12 bits) padded with 0000(4 bits)), and compare with the Cell Id returned in the Additional Textcd /opt/bin./BSGCLI.execd FGW:<DNNumber>;get {globalRNCIdRncId};Change the information in the registration request or the BSR DATA XML file to be in sync and perform the registration again.		

Table 28-170 BSG_imsiDirectoryFull

Alarm	Attributes	Applicable major release
Name: BSG_imsiDirectoryFull (5782) Type: qualityOfServiceAlarm Package: femto.BSG_imsiDirectoryFull Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the IMSI directory has become full and existing entries have been discarded to make space for new entries		
Remedial action: Perform a UE de-registration to check whether the alarm is auto cleared.If Step 1 does not resolve the issue, de-register Small Cells and check whether alarm is auto cleared.The mentioned IMSI directory is an internal BSR Gateway data structure, and the BSR Gateway auto clears the alarm when the count in the directory is below the maximum limit.The IMSI directory limit is a MIM parameter imsidirectorymaximumentries.		

Table 28-171 BSG_incomingHoProvisionError

Alarm	Attributes	Applicable major release
Name: BSG_incomingHoProvisionError (5783) Type: processingErrorAlarm Package: femto.BSG_incomingHoProvisionError Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised if the Target BSR Selection Algorithm has incorrect data provisioned for incoming HO on a particular RAT, when incoming HO isenabled for that RAT,		
Remedial action: This fault is manually cleared from the OAM system.Configure the Small Cell with correct data (for example, basic, virtual or enhanced configuration) for incoming HO, on the particular RAT. Refer SRS-BSG-CP-1222, SRS-BSG-CP-1223, SRS-BSG-CP-1224, and SRS-BSG-CP-1225 for configurations.		

Table 28-172 BSG_invalidBSRIdInBSRRegistrationMessage

Alarm	Attributes	Applicable major release
Name: BSG_invalidBSRIdInBSRRegistrationMessage (5784) Type: communicationsAlarm Package: femto.BSG_ invalidBSRIdInBSRRegistrationMessage Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives BSR registration message with already registered BSR ID and different IP Sec address		
Remedial action: This alarm is cleared by registering the Small Cell with a BSR ID, which does not exist in the BSR Gateway.The successful registration is verified in the BSR Gateway console, using the command bsg_get_bsr_registrations.		

Table 28-173 BSG_invalidMocnConfiguration

Alarm	Attributes	Applicable major release
Name: BSG_invalidMocnConfiguration (5785) Type: processingErrorAlarm Package: femto.BSG_invalidMocnConfiguration Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm shall be raised when CS or PS region is not assigned or CN Node for selected operator is not configured in the region for split NRIs based MOCN operator selection		
Remedial action: Check the MOCN configuration planning		

Table 28-174 BSG_macroLacRacNotAllowed

Alarm	Attributes	Applicable major release
Name: BSG_macroLacRacNotAllowed (5786) Type: processingErrorAlarm Package: femto.BSG_macroLacRacNotAllowed Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Femto registration contains a Macro LAC RAC that is not allowed by this Femto.		
Remedial action: This alarm is cleared manually from the OAM system when BSG is configured with macro LAC RAC and accepts new registration requests from Small Cell.		

Table 28-175 BSG_manuallyAssignedPSCConflicts

Alarm	Attributes	Applicable major release
Name: BSG_manuallyAssignedPSCConflicts (8466) Type: processingErrorAlarm Package: femto.BSG_manuallyAssignedPSCConflicts Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: A Grid Access Point in the Femto Group has been manually assigned a PSC which conflicts with the assignment of the other Access Points.		
Remedial action: Change the Manual PSC of the AP or perform self optimisation of the conflicting APs.		

Table 28-176 BSG_massBsrCsCnConnLost

Alarm	Attributes	Applicable major release
Name: BSG_massBsrCsCnConnLost (5787) Type: communicationsAlarm Package: femto.BSG_massBsrCsCnConnLost Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteNodeTransmissionError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: A significant number of Femto BSRs have detected a loss of connectivity to the CS Core Network, even though their transport layer is still connected.		
Remedial action: The alarm is automatically cleared by the clear alarmBSG_MASSBSRCSCNCONNLOSTCLEARANCE.2. The PM counter difference between CS SCCP Req attempts and success willindicate CS core network connectivity issue.3. Investigate the fault at the MSC side.4. The alarm is cleared by de-registering the registered Femtocells, so that the sizereduces and is lesser than the threshold level.5. If the problem persists, contact Nokia customer support.		

Table 28-177 BSG_massBsrOutOfService

Alarm	Attributes	Applicable major release
Name: BSG_massBsrOutOfService (5788) Type: equipmentAlarm Package: femto.BSG_massBsrOutOfService Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is triggered when the number of active bsrOutOfService alarms reaches the threshold defined by the BSG:: maxNumBSRServiceAlarms attribute		
Remedial action: The alarm is automatically detected and cleared by the BSR Gateway, when the total number of failed Small Cells drops below the BSG:: maxNumBSRServiceAlarms value.The value of the attribute, maxNumBSRServiceAlarms can be set with the BSGCLI in the class BSR Gateway. Execute the following commands in the BSGCLI:./BSGCLI.exe, to run the BSGCLI exe.cd FGW:<FGW Instance Number>cd BSG:<BSG Instance Number>set {maxNumBSRServiceAlarms="<Threshold value>}"		

Table 28-178 BSG_maximumImsiListThresholdExceeded

Alarm	Attributes	Applicable major release
Name: BSG_maximumImsiListThresholdExceeded (5789) Type: qualityOfServiceAlarm Package: femto.BSG_ maximumImsiListThresholdExceeded Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the number of IMSIs in the ACL lists defined on the SCGW has exceeded the maximum threshold defined by attribute maximumIMSIList. The alarm is automatically cleared whenever the number falls below this threshold.		
Remedial action: The operator must do a manual clearance.This alarm gets cleared when total number of IMSIs in the ACL lists defined on the SCGW falls below the maximumIMSIList value.		

Table 28-179 BSG_maximumPSCAssignmentAlarmsRaised

Alarm	Attributes	Applicable major release
Name: BSG_maximumPSCAssignmentAlarmsRaised (8467) Type: processingErrorAlarm Package: femto.BSG_ maximumPSCAssignmentAlarmsRaised Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: The maximum number of PSC Assignment alarms have been raised		
Remedial action: Check and resolve the existing PSC assignment related alarms		

Table 28-180 BSG_minimumImsiListThresholdExceeded

Alarm	Attributes	Applicable major release
Name: BSG_minimumImsiListThresholdExceeded (5790) Type: qualityOfServiceAlarm Package: femto.BSG_ minimumImsiListThresholdExceeded Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the number of IMSIs in the ACL lists defined on the SCGW has exceeded the minimum threshold defined by attribute minimumIMSIList. The alarm is automatically cleared whenever the number falls below this threshold.		
Remedial action: The operator must do a manual clearance.This alarm gets cleared when total number of IMSIs in the ACL lists defined on the BSR Gateway falls below the minimumIMSIList value.		

Table 28-181 BSG_newBSRRegistrationRejectedDueToOverload

Alarm	Attributes	Applicable major release
Name: BSG_ newBSRRegistrationRejectedDueToOverload (5791) Type: qualityOfServiceAlarm Package: femto.BSG_ newBSRRegistrationRejectedDueToOverload Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW rejects new BSR registration due to overload		
Remedial action: This fault is automatically cleared by the Clear Alarm BSG_ NEWBSRREGISTRATIONACCEPTEDAFTERRECOVERFROMOVERLOAD.The alarm is cleared when the BSR Gateway recovers from the overload condition.The %CPU column of top command can be used to check the CPU utilization.The memory utilization can be checked, by using the command freeFree memory specified should be high. compared to the used memory available, for recovering to normal overload.The used buffer cache memory should be low.To drop the cache memory use the command echo 3> /proc/sys/vm/ drop_caches.Terminate some calls to check whether memory utilization comes down, clearing the alarm.If the memory utilization does not reduce and the alarm persists, de-register the Small Cells and check for reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforced Small Cell de-registration. Enforce a BSR Gateway switch-over by terminating the BSR Gateway application.If the problem persists, contact Nokia customer support.		

Table 28-182 BSG_newRANAPCallRejectedDueToOverload

Alarm	Attributes	Applicable major release
Name: BSG_newRANAPCallRejectedDueToOverload (5792) Type: qualityOfServiceAlarm Package: femto.BSG_ newRANAPCallRejectedDueToOverload Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW rejects RANAP calls due to overload		
Remedial action: This fault is automatically cleared by the Clear Alarm BSG_OVERLOADCONDITIONBACKTONORMAL.The alarm is cleared when the BSR Gateway recovers from the overload condition.The %CPU column of top command can be used to check the CPU utilization.Enter the command free to check the memory utilization:Free memory specified should be high. compared to the used memory available, for recovering to normal overload.The used buffer cache memory should be low.To drop the cache memory use the command echo 3 >/proc/sys/vm/drop_caches.Terminate some calls to check whether memory utilization comes down, clearing the alarm.If the memory utilization does not reduce and the alarm persists, de-register the Small Cells and check for reduction in memory utilization.If there is no reduction in memory utilization, even after call termination and enforced Small Cell de-registration. Enforce a BSR Gateway switch-over by terminating the BSR Gateway application.If the problem persists, contact Nokia customer support.		

Table 28-183 BSG_pagingRecordLimitExceeded

Alarm	Attributes	Applicable major release
Name: BSG_pagingRecordLimitExceeded (5793) Type: processingErrorAlarm Package: femto.BSG_pagingRecordLimitExceeded Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the number of Paging messages for the same Macro LAC RAC per Batch has exceded its limit.		
Remedial action: This alarm is cleared automatically from the OAM system when the number of paging records for a macro LAC RACin a BSGPP messages is lower than 256 after the sustain period configured from the BSG.		

Table 28-184 BSG_provisionedBSRsThresholdExceeded

Alarm	Attributes	Applicable major release
Name: BSG_provisionedBSRsThresholdExceeded (12966) Type: equipmentAlarm Package: femto.BSG_ provisionedBSRsThresholdExceeded Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • SC19.1 • SC20.1
Description: This alarm is triggered when the number of provisioned BSRs exceeds FGW threshold limit of 65535.		
Remedial action: Check if more than 65535 (FGW threshold limit) entries are being sent in the BSR data file to FGW from the OAM system. If yes take steps to limit the provisioning to 65535 for the cluster.The operator must do a manual clearance for the alarm.		

Table 28-185 BSG_pSCAssignmentCapacityExhausted

Alarm	Attributes	Applicable major release
Name: BSG_pSCAssignmentCapacityExhausted (8468) Type: processingErrorAlarm Package: femto.BSG_ pSCAssignmentCapacityExhausted Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: An Access Point in the Femto Group has requested a PSC, but the SCGW has not been able to assign a unique one based on the group configuration		
Remedial action: Check the Access Point and Femto Group configuration to allocate additional PSCs if possible.		

Table 28-186 BSG_pSCAssignmentDuplicatedInGroup

Alarm	Attributes	Applicable major release
Name: BSG_pSCAssignmentDuplicatedInGroup (8469) Type: processingErrorAlarm Package: femto.BSG_ pSCAssignmentDuplicatedInGroup Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: An Access Point which is marked as needing a unqiue PSC in the group has been assigned aPSC which is duplicated in the group.		
Remedial action: Perform a self-optmisation for the BSR identified in the additional information for this alarm at the next oppotunity.		

Table 28-187 BSG_pscInconsistent

Alarm	Attributes	Applicable major release
Name: BSG_pscInconsistent (5794) Type: processingErrorAlarm Package: femto.BSG_pscInconsistent Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised if PSC consistency is not maintained at BSR registration for open access BSR with incoming HO enabled.		
Remedial action: Check for psctype in the attribute bsrPSCforVirtEnhCellid.If closed access and the incoming HO is open, check the Small Cell and identify the root cause of the issue.If open access and the incoming HO is closed, check the Small Cell and identify the root cause of the issue.If the incoming HO mode matches with the MIM attribute mode, then this alarm has to be manually cleared at the OAM system..If BSR Gateway raises this alarm even in matching case, contact Nokia customer support.This alarm is cleared manually.		

Table 28-188 BSG_ranapPagingHighRateExceded

Alarm	Attributes	Applicable major release
Name: BSG_ranapPagingHighRateExceded (5795) Type: processingErrorAlarm Package: femto.BSG_ranapPagingHighRateExceded Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the number of RANAP Paging messages per second received has exceded its High limit. RANAP Paging messages above this limit shall be dropped.		
Remedial action: This alarm is cleared automatically from the OAM system when the number of RANAP paging messages processedper second is lower than the paging overload high value defined in BSGclass, after sustain period configured in the BSG.		

Table 28-189 BSG_ranapPagingLowRateExceded

Alarm	Attributes	Applicable major release
Name: BSG_ranapPagingLowRateExceded (5796) Type: processingErrorAlarm Package: femto.BSG_ranapPagingLowRateExceded Raised on class: femto.BSG	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the number of RANAP Paging messages per second received has exceded its Low limit.		
Remedial action: This alarm is cleared automatically from the OAM system when the number of RANAP paging messages processedper second is lower than the paging overload low value defined in the BSG class after sustain period configured in the BSG.		

Table 28-190 BSG_rangeOfStreamIdFromMSCNotSupported

Alarm	Attributes	Applicable major release
Name: BSG_rangeOfStreamIdFromMSCNotSupported (5797) Type: communicationsAlarm Package: femto.BSG_ rangeOfStreamIdFromMSCNotSupported Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives RANAP message with invalid stream ID on the SCTP association from the 3G-MSC		
Remedial action: This alarm is cleared only if the streams are available for establishment of a call.The streams are freed by terminating the mobile originated calls.		

Table 28-191 BSG_rangeOfStreamIdNotSupported

Alarm	Attributes	Applicable major release
Name: BSG_rangeOfStreamIdNotSupported (5798) Type: communicationsAlarm Package: femto.BSG_rangeOfStreamIdNotSupported Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives STRMGR PDU with invalid stream ID from the BSR		
Remedial action: This fault is cleared manually from the OAM system.This alarm is cleared by providing Stream ID between 0 and 255 in the Small Cell, while executing the calls.		

Table 28-192 BSG_receivedInvalidBSRRegistrationMessage

Alarm	Attributes	Applicable major release
Name: BSG_receivedInvalidBSRRegistrationMessage (5799) Type: communicationsAlarm Package: femto.BSG_ receivedInvalidBSRRegistrationMessage Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives invalid BSR registration message from BSR		
Remedial action: Check using wireshark or ethereal traces whether any invalid IE is sent as part of Small Cell registration request.Check Fatal/Error logs in Log_FMG.log file with respect to decoding of Small Cell registration request.Use the above information to isolate the issue at Small Cell or BSR Gateway end.This alarm is cleared manually from the OAM system when a valid Small Cell registration request is received by the BSR Gateway.		

Table 28-193 BSG_registrationOfBSRFailed

Alarm	Attributes	Applicable major release
Name: BSG_registrationOfBSRFailed (5800) Type: processingErrorAlarm Package: femto.BSG_registrationOfBSRFailed Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to register a valid BSR registration request due to some configuration errors in SCGW		
Remedial action: This fault is cleared manually from the OAM system.The alarm is cleared by registering Small Cell with the following valid registration elements:BSG_GWY_PRM_BSR_IDBSG_GWY_PRM_LACBSG_GWY_PRM_UC_IDBSG_GWY_PRM_RACBSR_ GWY_PRM_FEMTO_INTERNET_PUBLIC_IP_ADDRBSR_GWY_PRM_BSR_GROUP_IDBSR_GWY_PRM_BSR_ CAPABILITIES1BSR_GWY_PRM_BSR_FACTORY_SERIAL_NUMBERBSR_GWY_PRM_BSR_REG_REASONBSG_GWY_PRM_ GEO_LOCATIONBSR_GWY_BSRPSCBSR_GWY_UMTS_VIRTCIDBSR_GWY_GSM_VIRTCIDBSR_GWY_UMTS_ MACROCELINFOBSR_GWY_UMTS_MACROCELINFOThe successful registration of a Small Cell can be verified in the BSGConsole, using the command bsg_get_bsr_registrations.		

Table 28-194 BSG_spareAlarmBSGADAC1

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC1 (12979) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC1 Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm		

Table 28-195 BSG_spareAlarmBSGADAC2

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC2 (12980) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC2 Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm		

Table 28-196 BSG_spareAlarmBSGADAC3

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC3 (12981) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC3 Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm		

Table 28-197 BSG_spareAlarmBSGADAC4

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC4 (12982) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC4 Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm		

Table 28-198 BSG_spareAlarmBSGADAC5

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC5 (12983) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC5 Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm		

Table 28-199 BSG_spareAlarmBSGADAC6

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADAC6 (12984) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADAC6 Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm		

Table 28-200 BSG_spareAlarmBSGADMC1

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC1 (12985) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC1 Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm		

Table 28-201 BSG_spareAlarmBSGADMC2

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC2 (12986) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC2 Raised on class: femto.BSG	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm		

Table 28-202 BSG_spareAlarmBSGADMC3

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC3 (12987) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC3 Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm		

Table 28-203 BSG_spareAlarmBSGADMC4

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC4 (12988) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC4 Raised on class: femto.BSG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm		

Table 28-204 BSG_spareAlarmBSGADMC5

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC5 (12989) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC5 Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm		

Table 28-205 BSG_spareAlarmBSGADMC6

Alarm	Attributes	Applicable major release
Name: BSG_spareAlarmBSGADMC6 (12990) Type: processingErrorAlarm Package: femto.BSG_spareAlarmBSGADMC6 Raised on class: femto.BSG	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm		

Table 28-206 BVG_noBvgMapping

Alarm	Attributes	Applicable major release
Name: BVG_noBvgMapping (5860) Type: processingErrorAlarm Package: femto.BVG_noBvgMapping Raised on class: femto.BVG	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-206 BVG_noBvgMapping (continued)

Alarm	Attributes	Applicable major release
Description: This fault is generated when the BVG function receives a user plane packet which gets discarded due to there being no associated binding in the BVG mapping table.		
Remedial action: This alarm is generated when the BVG application receives a (user plane) voice packet, which gets discarded, due to there being no voice connection between the Small Cell and BTG.To determine the Small Cell, for which the alarm is raised, use the Log_ BTG.log file, located at /opt/log/BTG/. Use the pattern BVG_NOBVGMAPPING Alarm raised for BSR.Initiate a voice call between the Small Cell and core network. Verify the the connection is established between the Small Cell and BTG through BTGConsole. Run BTGConsole application and enter btg_get_bvg_table. A rule should be present for the corresponding Small Cell and core network.		

Table 28-207 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 28-208 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 28-209 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 28-210 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 28-211 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		

Table 28-211 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 28-212 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 28-213 CPUInfo_configErrorAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_configErrorAssert (5884) Type: equipmentAlarm Package: femto.CPUInfo_configErrorAssert Raised on class: femto.FGWCPUInfo	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Configuration error assert		
Remedial action: Check the BIOS processor configuration.Rectify the processor configuration if there are issues.Reboot the system after making the BIOS configuration changes.After receiving the CPUInfo_configErrorDeassert alarm, the operator can do a manual clearance.		

Table 28-214 CPUInfo_configErrorDeassert

Alarm	Attributes	Applicable major release
Name: CPUInfo_configErrorDeassert (5885) Type: equipmentAlarm Package: femto.CPUInfo_configErrorDeassert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Configuration error de-assert		
Remedial action: The operator must do a manual clearance.		

Table 28-215 CPUInfo_disabledAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_disabledAssert (5886) Type: equipmentAlarm Package: femto.CPUInfo_disabledAssert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Disabled assert		
Remedial action: Check the BIOS configuration for CPU configuration issue.Check the system CPU cooling for overheat related issues.Check if the processor has been inserted in the slot appropriately.Reboot the system after performing the corrective action.After receiving the CPUInfo_disabledDeassert alarm, the operator can do a manual clearance.		

Table 28-216 CPUInfo_disabledDeassert

Alarm	Attributes	Applicable major release
Name: CPUInfo_disabledDeassert (5887) Type: equipmentAlarm Package: femto.CPUInfo_disabledDeassert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Disabled de-assert		
Remedial action: The operator must do a manual clearance.		

Table 28-217 CPUInfo_iERRAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_iERRAssert (5888) Type: equipmentAlarm Package: femto.CPUInfo_iERRAssert Raised on class: femto.FGWCPUInfo	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: IERR assert		
Remedial action: Check the cooling system to ensure that, proper cooling for the processor is in place.Check whether the processor is properly secured in its slot.Reboot the system after verifying and correcting issues identified in steps 1 and 2.After receiving the CPUInfo_iERRDeassert alarm, the operator must do a manual clearance.		

Table 28-218 CPUInfo_iERRDeassert

Alarm	Attributes	Applicable major release
Name: CPUInfo_iERRDeassert (5889) Type: equipmentAlarm Package: femto.CPUInfo_iERRDeassert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: IERR de-assert		
Remedial action: No action needed. CPU problem is recovered.		

Table 28-219 CPUInfo_presenceAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_presenceAssert (5890) Type: physicalViolation Package: femto.CPUInfo_presenceAssert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence assert		
Remedial action: The operator must do a manual clearance.		

Table 28-220 CPUInfo_presenceDeassert

Alarm	Attributes	Applicable major release
Name: CPUInfo_presenceDeassert (5891) Type: physicalViolation Package: femto.CPUInfo_presenceDeassert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence de-assert		
Remedial action: Check the BIOS configuration for CPU configuration issue.Check the system CPU cooling for overheat related issues.Check if the processor is properly secured in its slot.After receiving the CPUInfo_presenceAssert alarm, the operator can do a manual clearance.		

Table 28-221 CPUInfo_thermakTripAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_thermakTripAssert (5892) Type: equipmentAlarm Package: femto.CPUInfo_thermakTripAssert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Thermal trip assert		
Remedial action: NA		

Table 28-222 CPUInfo_thermalTripAssert

Alarm	Attributes	Applicable major release
Name: CPUInfo_thermalTripAssert (5893) Type: equipmentAlarm Package: femto.CPUInfo_thermalTripAssert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1
Description: Thermal trip assert		
Remedial action: Check the cooling system to ensure, that proper cooling for the processor is in place.Check whether the processor is properly secured in its slot.Reboot the system after verifying and correcting issues identified in steps 1 and 2.		

Table 28-223 CPUInfo_thermalTripDeassert

Alarm	Attributes	Applicable major release
Name: CPUInfo_thermalTripDeassert (5894) Type: equipmentAlarm Package: femto.CPUInfo_thermalTripDeassert Raised on class: femto.FGWCPUInfo	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: processorProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Thermal trip de-assert		
Remedial action: No action needed. CPU problem is recovered.		

Table 28-224 CPU_memTempMajor

Alarm	Attributes	Applicable major release
Name: CPU_memTempMajor (5895) Type: equipmentAlarm Package: femto.CPU_memTempMajor Raised on class: femto.CPU	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Memory temperature Major		
Remedial action: Check system temperature and cooling		

Table 28-225 CPU_presenceAssert

Alarm	Attributes	Applicable major release
Name: CPU_presenceAssert (5896) Type: physicalViolation Package: femto.CPU_presenceAssert Raised on class: femto.CPU	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence assert		
Remedial action: Clear the alarms manually from the OAM system after replacing the hardware.		

Table 28-226 CPU_presenceDeassert

Alarm	Attributes	Applicable major release
Name: CPU_presenceDeassert (5897) Type: physicalViolation Package: femto.CPU_presenceDeassert Raised on class: femto.CPU	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence de-assert		
Remedial action: Clear the alarms manually from the OAM system after replacing the hardware.		

Table 28-227 CPU_tempCritical

Alarm	Attributes	Applicable major release
Name: CPU_tempCritical (5898) Type: equipmentAlarm Package: femto.CPU_tempCritical Raised on class: femto.CPU	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Temperature Critical		
Remedial action: Clear the alarms manually from the OAM system after replacing the hardware.For further assistance, contact Nokia customer support		

Table 28-228 CPU_tempMajor

Alarm	Attributes	Applicable major release
Name: CPU_tempMajor (5899) Type: equipmentAlarm Package: femto.CPU_tempMajor Raised on class: femto.CPU	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Temperature Major		
Remedial action: Check system temperature and cooling		

Table 28-229 CsRegion_invalidSuperLacOverlap

Alarm	Attributes	Applicable major release
Name: CsRegion_invalidSuperLacOverlap (5900) Type: integrityViolation Package: femto.CsRegion_invalidSuperLacOverlap Raised on class: femto.CsRegion	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Incorrect configuration for superLAC values which have different superLACs for overlapping regions.		
Remedial action: Check the BSG configuration OAM_Preconfig.xml file and make sure the CSRegion and superLAC configurations are correct.		

Table 28-230 DimmSlot_deviceInstalledAssert

Alarm	Attributes	Applicable major release
Name: DimmSlot_deviceInstalledAssert (5903) Type: equipmentAlarm Package: femto.DimmSlot_deviceInstalledAssert Raised on class: femto.DimmSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Device installed assert		
Remedial action: The operator must do a manual clearance.		

Table 28-231 DimmSlot_disabledAssert

Alarm	Attributes	Applicable major release
Name: DimmSlot_disabledAssert (5904) Type: equipmentAlarm Package: femto.DimmSlot_disabledAssert Raised on class: femto.DimmSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Disabled assert		
Remedial action: Check the BIOS configuration for CPU configuration issue.Check the system CPU cooling for overheat related issues.Check if the processor has been inserted in the slot appropriately.Reboot the system after performing the corrective action.After receiving the CPUInfo_disabledDeassert alarm, the operator can do a manual clearance.		

Table 28-232 DimmSlot_faultStatusAssert

Alarm	Attributes	Applicable major release
Name: DimmSlot_faultStatusAssert (5905) Type: equipmentAlarm Package: femto.DimmSlot_faultStatusAssert Raised on class: femto.DimmSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Fault status assert		
Remedial action: Check whether there are misalignments in the Dimmslot.Check whether the memory card is properly inserted in the Dimmslot.Reboot the system after rectifying the above mentioned issuesPerform a manual clearance.		

Table 28-233 DimmSlot_sparingAssert

Alarm	Attributes	Applicable major release
Name: DimmSlot_sparingAssert (5906) Type: equipmentAlarm Package: femto.DimmSlot_sparingAssert Raised on class: femto.DimmSlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Sparing assert		
Remedial action: Check whether there are misalignments in the DimmSlot.Check whether the memory card is properly inserted in the DimmSlot.Reboot the system after rectifying the above mentioned issues.Perform manual clearance.		

Table 28-234 DiskPartition_partitionNearingCapacity

Alarm	Attributes	Applicable major release
Name: DiskPartition_partitionNearingCapacity (8477) Type: equipmentAlarm Package: femto.DiskPartition_partitionNearingCapacity Raised on class: femto.DiskPartition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the disk usage has exceeded upper threshold . The alarm is automatically cleared whenever disk usage is reduced below lower threshold.		
Remedial action: Check or correct the disk usage in the identified partition.		

Table 28-235 DNS_dnsServerDownNode1

Alarm	Attributes	Applicable major release
Name: DNS_dnsServerDownNode1 (5901) Type: processingErrorAlarm Package: femto.DNS_dnsServerDownNode1 Raised on class: femto.DNS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the DNS server within SCGW hardware Node1 is out of service.		
Remedial action: Enter the command ps -ef | grep named to verify whether the DNS service is running on the BSR Gateway server.		

Table 28-236 DNS_dnsServerDownNode2

Alarm	Attributes	Applicable major release
Name: DNS_dnsServerDownNode2 (5902) Type: processingErrorAlarm Package: femto.DNS_dnsServerDownNode2 Raised on class: femto.DNS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the DNS server within SCGW hardware Node2 is out of service.		
Remedial action: Enter the command ps -ef | grep named to verify whether the DNS service is running on the BSR Gateway server.		

Table 28-237 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 28-238 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 28-239 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 28-240 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		

Table 28-240 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 28-241 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 28-242 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 28-243 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 28-244 EthernetIntf_interfaceActive

Alarm	Attributes	Applicable major release
Name: EthernetIntf_interfaceActive (5907) Type: communicationsAlarm Package: femto.EthernetIntf_interfaceActive Raised on class: femto.EthernetIntf	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the EthernetIntf interface is up		
Remedial action: The operator must do a manual clearance.		

Table 28-245 EthernetIntf_interfaceFailure

Alarm	Attributes	Applicable major release
Name: EthernetIntf_interfaceFailure (5908) Type: equipmentAlarm Package: femto.EthernetIntf_interfaceFailure Raised on class: femto.EthernetIntf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when a EthernetIntf interface failure occurs		
Remedial action: The alarm gets cleared automatically by the clear alarmETHERNETINTF_INTERFACEFAILURECLEARANCE, once the connectivity is restored.Check if the ethernet interface on BONO is up and running.If the problem persists, contact Nokia customer support.		

Table 28-246 EthernetPort_cardFailure

Alarm	Attributes	Applicable major release
Name: EthernetPort_cardFailure (5909) Type: equipmentAlarm Package: femto.EthernetPort_cardFailure Raised on class: femto.EthernetPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when EthernetPort card failure occurs		
Remedial action: Check whether the Ethernet card to be installed in the X4250 system, is recommended by SUN.Check whether the PCIe Ethernet card is inserted in the appropriate slot.Check whether there are any alignment issues while installing the Ethernet card.Rectify the problems and reboot the system.Connect the cable to the card and check whether the LED is blinking, indicating flow of traffic.After receiving EthernetPort_cardFailure clearance alarm, the operator must do a manual clearance.		

Table 28-247 EthernetPort_interfaceActive

Alarm	Attributes	Applicable major release
Name: EthernetPort_interfaceActive (5910) Type: communicationsAlarm Package: femto.EthernetPort_interfaceActive Raised on class: femto.EthernetPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when EthernetPort interface is up		
Remedial action: The operator must do a manual clearance.		

Table 28-248 ExternalEthernetIntfPort_interfaceActive

Alarm	Attributes	Applicable major release
Name: ExternalEthernetIntfPort_interfaceActive (5911) Type: communicationsAlarm Package: femto.ExternalEthernetIntfPort_ interfaceActive Raised on class: femto.ExternalEthernetIntfPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the EthernetIntf interface is up		
Remedial action: The operator must do a manual clearance.		

Table 28-249 ExternalEthernetIntfPort_interfaceFailure

Alarm	Attributes	Applicable major release
Name: ExternalEthernetIntfPort_interfaceFailure (5912) Type: equipmentAlarm Package: femto.ExternalEthernetIntfPort_ interfaceFailure Raised on class: femto.ExternalEthernetIntfPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when an external EthernetIntf interface failure occurs		
Remedial action: Check the RTM port status on the chassis and on the Malban.Ensure the RTM ports are up.This fault is cleared automatically by the clear alarmEXTERNALETHERNETINTFPORT_INTERFACEFAILURECLEARANCE.If the problem persists, contact Nokia customer support		

Table 28-250 FGW_aclViolation

Alarm	Attributes	Applicable major release
Name: FGW_aclViolation (5913) Type: securityServiceOrMechanismViolation Package: femto.FGW_aclViolation Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unauthorizedAccessAttempt	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW has detected a UE trying to get access to the network through a restricted closed access BSR even if the IMSI of the user is not listed in the ACL of the BSR.		
Remedial action: Check whether the IMSI is present in the ACL list of any Small Cell.If the IMSI is not present, then configure the Small Cell ACL list to include the IMSI.Perform actbsrdata upgrade from the OAM system and sync the new BSR DATA XML file with the BSR GatewayRetest the scenario.		

Table 28-251 FGW_activeFGWOAMPortFailure

Alarm	Attributes	Applicable major release
Name: FGW_activeFGWOAMPortFailure (5914) Type: communicationsAlarm Package: femto.FGW_activeFGWOAMPortFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that 1G port that is being used by SCGW OAM function has failed and SCGW shall start using other port for OAM function		
Remedial action: Investigate the cause of the 1G port failure in active FGW.This fault is automatically cleared by the alarmFGW_ ACTIVEFGWOAMPORTFAILURECLEARANCE.If the problem persists, contact Nokia customer support..		

Table 28-252 FGW_agpsServiceUnavailable

Alarm	Attributes	Applicable major release
Name: FGW_agpsServiceUnavailable (5915) Type: communicationsAlarm Package: femto.FGW_agpsServiceUnavailable Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is raised if the Assisted GPS Service is unavailable		
Remedial action: Check the AGPS system configuration and connectivity to the AGPS server.		

Table 28-253 FGW_automaticFailoverInitiatedByActiveNode

Alarm	Attributes	Applicable major release
Name: FGW_automaticFailoverInitiatedByActiveNode (5916) Type: processingErrorAlarm Package: femto.FGW_ automaticFailoverInitiatedByActiveNode Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated whenever a failover is initiated by the active node due to the detection of a failure within the node,		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-254 FGW_automaticFailoverInitiatedByStandbyNode

Alarm	Attributes	Applicable major release
Name: FGW_ automaticFailoverInitiatedByStandbyNode (5917) Type: processingErrorAlarm Package: femto.FGW_ automaticFailoverInitiatedByStandbyNode Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated whenever a failover is initiated by the standby node due to the detection of a failure within the node,		
Remedial action: NA		

Table 28-255 FGW_availabilityTargetAchieved

Alarm	Attributes	Applicable major release
Name: FGW_availabilityTargetAchieved (5918) Type: processingErrorAlarm Package: femto.FGW_availabilityTargetAchieved Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated following a failover when the the newly-active node has bound the floating IP address(es) for FAP connection, and it has sent out the 'Notify Connection Status (Active)' message to all femtos which have SCTP associations to the fixed IP address.		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-256 FGW_baseboardControllerFailure

Alarm	Attributes	Applicable major release
Name: FGW_baseboardControllerFailure (5919) Type: equipmentAlarm Package: femto.FGW_baseboardControllerFailure Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised if the IPMI driver fails to start because it cannot communicate with the controller.		
Remedial action: Contact Nokia technical support for assistance.		

Table 28-257 FGW_bsrDataFileDownloadFailed

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataFileDownloadFailed (5920) Type: processingErrorAlarm Package: femto.FGW_bsrDataFileDownloadFailed Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW has failed to download a BSR Data file from the OAM system		
Remedial action: Verify the connectivity between the OAM system and the Gateway.Verify that the appropriate keys have been exchanged to enable automatic download between the BSR Gateway and the OAM system.Verify that the necessary file download permission is granted.Verify that the /opt/bsrdata directory is present in the system.		

Table 28-258 FGW_bsrDataFileEntryInvalid

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataFileEntryInvalid (12742) Type: processingErrorAlarm Package: femto.FGW_bsrDataFileEntryInvalid Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the FGW has detected that one or more BSR/HeNB entry in the Data File has an invalid format during partial or complete ACL sync operation.		
Remedial action: The Operator should investigate and correct such invalid BSR/HeNB entries and initiate a manual ACL sync to effect the data update at the FGW.		

Table 28-259 FGW_bsrDataFileInvalid

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataFileInvalid (5921) Type: processingErrorAlarm Package: femto.FGW_bsrDataFileInvalid Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW has detected that the format of the BSR Data File has an invalid XML format		
Remedial action: Verify that the XML file downloaded from the OAM system is syntactically correct. Check if there is any tag mismatch in the XML file.Download the corrected XML file again usingactbsrdata command.		

Table 28-260 FGW_bsrDataLost

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataLost (5922) Type: processingErrorAlarm Package: femto.FGW_bsrDataLost Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW has determined a failure has occurred with the complete BSR data held on the SCGW		
Remedial action: Download the complete BSR DATA XML file again, using theactbsrdata command.Perform Small Cell registration and verify if the registrations aresuccessful.		

Table 28-261 FGW_bsrDataNonExistingBSR

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataNonExistingBSR (5923) Type: processingErrorAlarm Package: femto.FGW_bsrDataNonExistingBSR Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW has detected that there changes requested in the BSR Data file relating to a non esisting BSR record.		
Remedial action: Verify that the BSR record exists in the BSR DATA XML file for which the change had been requested.If the BSR record is not present, then perform actbsrdata upgrade and create the BSR record in the BSR DATA XML file.Perform the changes on the BSR record which has been obtained from the actbsrdata upgrade.		

Table 28-262 FGW_bsrDataQueueFailure

Alarm	Attributes	Applicable major release
Name: FGW_bsrDataQueueFailure (5924) Type: processingErrorAlarm Package: femto.FGW_bsrDataQueueFailure Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW has received a actBSRData request from the OAM system and it still has a maximum number of previous requests being queued		
Remedial action: Reduce the frequency of BSR DATA sync-up between the OAM system and BSR Gateway from once in 3 minutes to once in 6 minutes.This provides time for the BSR Gateway to process previous commands and to free up the command queueRetry the sync-up and see if the problem persists.		

Table 28-263 FGW_bsrIdClash

Alarm	Attributes	Applicable major release
Name: FGW_bsrIdClash (5925) Type: operationalViolation Package: femto.FGW_bsrIdClash Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: callEstablishmentError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW has detected that another BSR tries to register with a BSR-Id already used by another BSR.		
Remedial action: Re-configure the Small Cell with a different BSR ID.Perform actbsrdata upgrade from the OAM system, and synchronize the new BSR DATA XML file with the BSR Gateway.Re-register the Small Cell.		

Table 28-264 FGW_bsrIntegrityCheckFailure

Alarm	Attributes	Applicable major release
Name: FGW_bsrIntegrityCheckFailure (5926) Type: securityServiceOrMechanismViolation Package: femto.FGW_bsrIntegrityCheckFailure Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authenticationFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated on receipt of a BSR Registration message from the BSR and the 'Registration Reason' IE is present and has the value 'Integrity Protection Failed		
Remedial action: Contact Nokia technical support for assistance.		

Table 28-265 FGW_bsrIntegrityViolation

Alarm	Attributes	Applicable major release
Name: FGW_bsrIntegrityViolation (5927) Type: securityServiceOrMechanismViolation Package: femto.FGW_bsrIntegrityViolation Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authenticationFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW has detected a mismatch between the registration parameters received from the BSR and the provisioned BSR parameters. At least one of the following parameters might have been manipulated:- BSR-Id,- Group-Id,- Access mode		
Remedial action: Verify, that the BSR ID, Group ID, access mode of the registered Small Cell and associated FSN, is same as present in BSR DATA XML fileIf there is any mismatch, configure the BSR DATA XML file with the correct values.Perform actbsrdata upgrade from the OAM system andsync the new BSR DATA file with the BSR Gateway.Re-register this Small Cell.		

Table 28-266 FGW_cellIdClash

Alarm	Attributes	Applicable major release
Name: FGW_cellIdClash (5928) Type: operationalViolation Package: femto.FGW_cellIdClash Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: callEstablishmentError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW has detected that another BSR tries to register with a Cell Id already used by another BSR.		
Remedial action: Ensure that the bsrId present in the/opt/bsrdata/OAM_BsrDataPersistentDB.txt for the incoming normal overloadHnbId is not associated with any other Hnb		

Table 28-267 FGW_cpuOverloadMaximumThreshold

Alarm	Attributes	Applicable major release
Name: FGW_cpuOverloadMaximumThreshold (5929) Type: equipmentAlarm Package: femto.FGW_ cpuOverloadMaximumThreshold Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cpuCyclesLimitExceeded	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the SCGW has detected that the maximum CPU overload threshold has been exceeded		
Remedial action: The FGW shall initiate the swictover to the standby card in order to continue provide service after a brief outage.For further assistance please contact NOKIA customer support.		

Table 28-268 FGW_cpuOverloadMinimumThreshold

Alarm	Attributes	Applicable major release
Name: FGW_cpuOverloadMinimumThreshold (5930) Type: equipmentAlarm Package: femto.FGW_cpuOverloadMinimumThreshold Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the SCGW has detected that the mimimum CPU overload threshold has been exceeded		
Remedial action: This alarm is cleared when either the measured load falls below the minimum threshold as a result of FGW corrective actions or rises above the maximum thresold. The %CPU column of the top command can be used to check the CPU utilization.For further assistance please contact NOKIA customer support.		

Table 28-269 FGW_failedCreatingDynamicTransport

Alarm	Attributes	Applicable major release
Name: FGW_failedCreatingDynamicTransport (5931) Type: processingErrorAlarm Package: femto.FGW_ failedCreatingDynamicTransport Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when dynamic creation of TCP transport fails.		
Remedial action: There is no explicit corrective procedure for this alarm.Once the dynamic creation of TPC transport is successful, this fault is cleared manually from the OAM system.		

Table 28-270 FGW_femtoMsgRateExceeded

Alarm	Attributes	Applicable major release
Name: FGW_femtoMsgRateExceeded (5932) Type: equipmentAlarm Package: femto.FGW_femtoMsgRateExceeded Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: retransmissionRateExcessive	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The message rate from a femto has been exceeded, resulting in dropped messages. This indicates a serious software flaw or a hacked femto.		
Remedial action: This alarm is raised when the message rate from a Small Cell exceeds and there is no explicit corrective procedure for this alarm.Once the BSR Gateway accepts the messages from the Small Cell,this fault is cleared manually from the OAM system.		

Table 28-271 FGW_fgw10GPortFailureAtNonResilientState

Alarm	Attributes	Applicable major release
Name: FGW_fgw10GPortFailureAtNonResilientState (5933) Type: communicationsAlarm Package: femto.FGW_ fgw10GPortFailureAtNonResilientState Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is generated to report failure of 10G port on BONO when the redundancy state of the system is Active_NonResilient, which means that there is a 10G port failure at a state where the other 10G port is already unavailable		
Remedial action: Investigate the cause of the 10G port failure in active FGW.This fault is automatically cleared by the clear alarmFGW_FGW10GPORTFAILUREATNONRESILIENTSTATECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-272 FGW_fgwActiveNonResilient

Alarm	Attributes	Applicable major release
Name: FGW_fgwActiveNonResilient (5934) Type: communicationsAlarm Package: femto.FGW_fgwActiveNonResilient Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is generated to report failure of 10G port on BONO OR failure of MALBAN when the redundancy state of the system is Active, which means that Active system has lost the redundant path and has become non-resilient		
Remedial action: Investigate the cause of the 10G port failure in active FGW.This fault is cleared automatically byFGW_ FGWACTIVENONRESILIENTCLEARANCE..If the problem persists, contact Nokia customer support		

Table 28-273 FGW_fgwActiveNotResponding

Alarm	Attributes	Applicable major release
Name: FGW_fgwActiveNotResponding (5935) Type: communicationsAlarm Package: femto.FGW_fgwActiveNotResponding Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that standby detected a fault with Active and a failover is being triggered		
Remedial action: Verify that the switch to standby is successful.Investigate the cause of the problem with the active system.This fault is cleared automatically byFGW_FGWACTIVENOTRESPONDINGCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-274 FGW_fgwNodeIsolated

Alarm	Attributes	Applicable major release
Name: FGW_fgwNodeIsolated (5936) Type: communicationsAlarm Package: femto.FGW_fgwNodeIsolated Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW Node gets isolated from mate SCGW-Node		
Remedial action: Check the cabling between the BSR Gateway and the mate node.Check the cabling between the BSR Gateway and the Central Router.Ensure that the port, which holds the connections to the router and mate BSRGateway, is blinking, indicating flow of traffic.Stop/Start BSR Gateway to check whether the connection is restored.If problem still persists, initiate switch-over.For further assistance please contact NOKIA customer support.		

Table 28-275 FGW_fgwNodeStateChangeActiveToStandby

Alarm	Attributes	Applicable major release
Name: FGW_fgwNodeStateChangeActiveToStandby (5937) Type: communicationsAlarm Package: femto.FGW_ fgwNodeStateChangeActiveToStandby Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when SCGW Node status changes from Active to Standby		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.To verify whether the current system is active, execute the script /opt/scripts/Status.sh.Once the system status is active, the operator can clear the alarm.		

Table 28-276 FGW_fgwNodeStateChangeStandbyToActive

Alarm	Attributes	Applicable major release
Name: FGW_fgwNodeStateChangeStandbyToActive (5938) Type: communicationsAlarm Package: femto.FGW_ fgwNodeStateChangeStandbyToActive Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when SCGW Node status changes from Standby to Active		
Remedial action: This is initiated as a part of switch-over and there is no explicit corrective procedure for this alarm.To verify if the current system is in an active state, execute the script /opt/scripts/Status.sh. Check the reports.Once the system status is active, the operator can clear the alarm.		

Table 28-277 FGW_fgwStandbyNonResilient

Alarm	Attributes	Applicable major release
Name: FGW_fgwStandbyNonResilient (5939) Type: communicationsAlarm Package: femto.FGW_fgwStandbyNonResilient Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is generated to report failure of 10G port on BONO OR failure of MALBAN when the redundancy state of the system is Standby, which means thatStandby system has lost the redundant path and has become non-resilient		
Remedial action: Investigate the cause of the 10G port alarm.		

Table 28-278 FGW_fgwStandbyNotResponding

Alarm	Attributes	Applicable major release
Name: FGW_fgwStandbyNotResponding (5940) Type: communicationsAlarm Package: femto.FGW_fgwStandbyNotResponding Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that Active detected a fault with Standby . This fault indicates that FGW is running in simplex mode		
Remedial action: Check that the standby node is running and that there is connectivity between the active and standby nodes via internodeLink1 and internodeLink2 IP addresses.This fault is cleared automatically by FGW_ FGWSTANDBYNOTRESPONDINGCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-279 FGW_fgwStandbyUnavailable

Alarm	Attributes	Applicable major release
Name: FGW_fgwStandbyUnavailable (5941) Type: communicationsAlarm Package: femto.FGW_fgwStandbyUnavailable Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alaram indicates that SCGW standby node is not available		
Remedial action: Investigate the cause of the peer node communication.This fault is cleared automatically by clear alarmFGW_ FGWSTANDBYUNAVAILABLECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-280 FGW_fgwToCentralRouterConnectionFailed

Alarm	Attributes	Applicable major release
Name: FGW_fgwToCentralRouterConnectionFailed (5942) Type: communicationsAlarm Package: femto.FGW_ fgwToCentralRouterConnectionFailed Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when connection between SCGW and Central Router fails		
Remedial action: Check if the eth2 cable is secure in the port.Check if the port light on the connected eth2 is blinking, indicating traffic.Check the cabling at the Central Router.Stop/Start BSR Gateway to check if the connection is restored.If the problem persists, initiate a switch-over.The BSR Gateway sends a clearance alarm when the connection is restored.For further assistance contact Nokia customer support.		

Table 28-281 FGW_fmsHardResetInitiated

Alarm	Attributes	Applicable major release
Name: FGW_fmsHardResetInitiated (5943) Type: equipmentAlarm Package: femto.FGW_fmsHardResetInitiated Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is triggered when hard reset is initiated in SCGW when it receives a hard reset request from the OAM system		
Remedial action: The fault is automatically cleared when the system is restarted.Execute the command /opt/scripts/showproc to verify the system status.For further assistance contact Nokia customer support.		

Table 28-282 FGW_fmsSoftResetInitiated

Alarm	Attributes	Applicable major release
Name: FGW_fmsSoftResetInitiated (5944) Type: equipmentAlarm Package: femto.FGW_fmsSoftResetInitiated Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is triggered when soft reset is initiated in SCGW when it receives a soft reset request from the OAM system		
Remedial action: The fault is automatically cleared when the system is restarted.Execute the command /opt/scripts/showproc to verify the system status.For further assistance contact Nokia customer support.		

Table 28-283 FGW_hnbSecurityViolation

Alarm	Attributes	Applicable major release
Name: FGW_hnbSecurityViolation (5945) Type: operationalViolation Package: femto.FGW_hnbSecurityViolation Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: callEstablishmentError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW has detected that a BSR is trying to send HNBAP or RUA messages with 'UE Context Id' that is registered by another BSR.		
Remedial action: The fault is automatically cleared when the system is restarted.		

Table 28-284 FGW_incorrectIPAddress

Alarm	Attributes	Applicable major release
Name: FGW_incorrectIPAddress (5946) Type: processingErrorAlarm Package: femto.FGW_incorrectIPAddress Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when BSR tries to connect to SCGW on a specific IP address and fails.		
Remedial action: The fault is automatically cleared when the system is restarted.		

Table 28-285 FGW_initialisationInProgress

Alarm	Attributes	Applicable major release
Name: FGW_initialisationInProgress (5947) Type: equipmentAlarm Package: femto.FGW_initialisationInProgress Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This event is triggered when the system starts initiazing itself after reset		
Remedial action: If the system is completely up, that is, initialization is completed after all the threads are spawned and the SIGTRAN stack is initialized, this alarm is cleared automatically.		

Table 28-286 FGW_initializeAcceptorFail

Alarm	Attributes	Applicable major release
Name: FGW_initializeAcceptorFail (5948) Type: processingErrorAlarm Package: femto.FGW_initializeAcceptorFail Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when IP Address entry in SCGW configuration is wrongly configured.		
Remedial action: Configure the IP address and execute the command /opt/script/status.sh to verify the system status.Clear the alarm manually from the OAM system if the IP configuration is successful.		

Table 28-287 FGW_invalidDownloadedConfiguration

Alarm	Attributes	Applicable major release
Name: FGW_invalidDownloadedConfiguration (5949) Type: equipmentAlarm Package: femto.FGW_ invalidDownloadedConfiguration Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised when the downloaded configuration is not valid.Scenaio-1: During downloadDB operation, if the xml file is corrupt (parsing fail).In this case, new configuration will not be used and GW continues to use the old configuration.Scenario-2: During downloadDB operation, if constraint checks fail.In this case, new configuration file will be used but alarm will be raised with additional text Constraints check failed on downloaded configuration from WMSScenario-3:During GW start/restart (which includes switchover), if the constraint check fails.In this case, new configuration file will be used but alarm wil be raised with additional text Constraints check failed on running configuration		
Remedial action: The operator must do a manual clearance of the alarm.For scenario 1, operator need to fix the problem and downloadDB againFor scenario 2,3 operator need to try to fix the reason of constraint check failure.		

Table 28-288 FGW_invalidIuflexConfiguration

Alarm	Attributes	Applicable major release
Name: FGW_invalidIuflexConfiguration (5950) Type: processingErrorAlarm Package: femto.FGW_invalidIuflexConfiguration Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when inconsistent/missing configuration data is detected for Iuflex NNSF function		
Remedial action: This alarm is cleared manually by doing CSRegion/PSRegion and BSGraiToPsRegion/BSGlaiToCsRegion configurations in the BSR Gateway with the same LAC/RAC, PLMNID, NRI values configured in the initial UE message fromthe Small Cell.If the alarm is raised due to region mismatch, then configure the corresponding LAC/RAC/PLMNID values in the BSR Gateway.If the alarm is raised due to NRI mismatch, configure an Iu interface with the NRI value to be matched in the BSR Gateway.The mismatch is identified in the Log_FMG.log file after initiating call from the Small Cell.		

Table 28-289 FGW_lag1ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag1ExceededSeventyPercent (5951) Type: communicationsAlarm Package: femto.FGW_lag1ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG1 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-290 FGW_lag1TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag1TrafficImbalance (5952) Type: communicationsAlarm Package: femto.FGW_lag1TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG1 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 1 is correct and the links are working		

Table 28-291 FGW_lag2ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag2ExceededSeventyPercent (5953) Type: communicationsAlarm Package: femto.FGW_lag2ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG2 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-292 FGW_lag2TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag2TrafficImbalance (5954) Type: communicationsAlarm Package: femto.FGW_lag2TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG2 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 2 is correct and the links are working		

Table 28-293 FGW_lag3ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag3ExceededSeventyPercent (5955) Type: communicationsAlarm Package: femto.FGW_lag3ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG3 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-294 FGW_lag3TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag3TrafficImbalance (5956) Type: communicationsAlarm Package: femto.FGW_lag3TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG3 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 3 is correct and the links are working		

Table 28-295 FGW_lag4ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag4ExceededSeventyPercent (5957) Type: communicationsAlarm Package: femto.FGW_lag4ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG4 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-296 FGW_lag4TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag4TrafficImbalance (5958) Type: communicationsAlarm Package: femto.FGW_lag4TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG4 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 4 is correct and the links are working		

Table 28-297 FGW_lag5ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag5ExceededSeventyPercent (5959) Type: communicationsAlarm Package: femto.FGW_lag5ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG5 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-298 FGW_lag5TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag5TrafficImbalance (5960) Type: communicationsAlarm Package: femto.FGW_lag5TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG5 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 5 is correct and the links are working		

Table 28-299 FGW_lag6ExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_lag6ExceededSeventyPercent (5961) Type: communicationsAlarm Package: femto.FGW_lag6ExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on LAG6 of the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Check the system configuration and provision additional members of the LAG to provide capacity.		

Table 28-300 FGW_lag6TrafficImbalance

Alarm	Attributes	Applicable major release
Name: FGW_lag6TrafficImbalance (5962) Type: communicationsAlarm Package: femto.FGW_lag6TrafficImbalance Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever there is a traffic imbalance on the LAG6 ports of the RTM unit		
Remedial action: Check the cabling for the ports associated with LAG 6 is correct and the links are working		

Table 28-301 FGW_logFileTransferFailure

Alarm	Attributes	Applicable major release
Name: FGW_logFileTransferFailure (11146) Type: securityServiceOrMechanismViolation Package: femto.FGW_logFileTransferFailure Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that the centralized log file management capability for a SC GW host is attempting to transfer a copy of log files to the repository bearing host and the transfer procedure failed. Upon the next successful transfer, the alarm is automatically cleared.		
Remedial action: Root cause analyze the source of the problem that is interfering with the file transfer process and resolve this issue.		

Table 28-302 FGW_malbanConnectionFailure

Alarm	Attributes	Applicable major release
Name: FGW_malbanConnectionFailure (5963) Type: equipmentAlarm Package: femto.FGW_malbanConnectionFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Malban connection failure		
Remedial action: The alarm is cleared automatically by the BSR Gateway by the clear alarmFGW_ MALBANCONNECTIONFAILURECLEARANCE when Malban is able to communicate with FGW/SHMC.Check if the MALBAN in the given slot (MALBAN-A in slot 7 or MALBAN-B in slot 8) is operational.If the problem persists, contact Nokia customer support.		

Table 28-303 FGW_malbanVlanCreationFailure

Alarm	Attributes	Applicable major release
Name: FGW_malbanVlanCreationFailure (5964) Type: equipmentAlarm Package: femto.FGW_malbanVlanCreationFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Malban VLAN creation failure		
Remedial action: When MALBAN comes up, FGW re-configures all VLANs towards the MALBAN and few VLAN re-configurations may fail during the flap, those failures get reported asFGW_malbanVlanCreationFailure alarm. Although the re-configuration will succeeded later when the BONO-to-MALBAN interface stabilizes.If after MALBAN reboot the re-configuration does not succeed then there will be other outage ADAC alarms such as: StandbyNotResponding (if internodelink vlan config failed) ActiveNotResponding (if internodelink vlan config failed) IuCS or IuPS ASP down (if Core Network vlan config failed) S1 link down (if MME S1 link vlan config failed) OAM link down (if OAM vlan config failed) bsrOutOfService or heNBOutOfService (if FemtoCP or HeNBCP vlan config failed)After MALBAN boots up and becomes operational the above outage ADAC alarms are not raised, FGW_malbanVlanCreationFailure ADMC alarm can be clearedmanually. There is no remedial action needed.Recommend ping malban IPs If MALBAN IP is not reachable then check MALBAN presence and its operationalstate. If MALBAN IP is reachable then try stopbsg + startbsg. If outage ADAC alarms still persist then probably issue exists with BONO->MALBAN configuration script or MALBAN HW/SW issue.If the problem persists, contact Nokia customer support.		

Table 28-304 FGW_manualFailoverInitiatedByActiveNode

Alarm	Attributes	Applicable major release
Name: FGW_manualFailoverInitiatedByActiveNode (5965) Type: processingErrorAlarm Package: femto.FGW_ manualFailoverInitiatedByActiveNode Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated whenever a failover is manually initiated on the active node,		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-305 FGW_manualFailoverInitiatedByStandbyNode

Alarm	Attributes	Applicable major release
Name: FGW_manualFailoverInitiatedByStandbyNode (5966) Type: processingErrorAlarm Package: femto.FGW_ manualFailoverInitiatedByStandbyNode Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-305 FGW_manualFailoverInitiatedByStandbyNode (continued)

Alarm	Attributes	Applicable major release
Description: This fault is generated whenever a failover is manually initiated on the standby node,		
Remedial action: NA		

Table 28-306 FGW_maximumImsiListThresholdExceeded

Alarm	Attributes	Applicable major release
Name: FGW_maximumImsiListThresholdExceeded (5967) Type: qualityOfServiceAlarm Package: femto.FGW_ maximumImsiListThresholdExceeded Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The number of IMSIs in the ACL lists defined on the SCGW has exceeded the maximum threshold defined by attribute FGW::maximumIMSIList		
Remedial action: The operator must do a manual clearance.This alarm gets cleared when total number of IMSIs in the ACL lists defined on the SCGW falls below the maximumIMSIList value.		

Table 28-307 FGW_memoryOverloadMaximumThreshold

Alarm	Attributes	Applicable major release
Name: FGW_memoryOverloadMaximumThreshold (5968) Type: equipmentAlarm Package: femto.FGW_ memoryOverloadMaximumThreshold Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfMemory	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the SCGW has detected that the maximum memory overload threshold has been exceeded		
Remedial action: The FGW shall initiate the swictover to the standby card in order to continue provide service after a brief outage.For further assistance please contact NOKIA customer support		

Table 28-308 FGW_memoryOverloadMinimumThreshold

Alarm	Attributes	Applicable major release
Name: FGW_memoryOverloadMinimumThreshold (5969) Type: equipmentAlarm Package: femto.FGW_ memoryOverloadMinimumThreshold Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-308 FGW_memoryOverloadMinimumThreshold (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised whenever the SCGW has detected that the mimimum memory overload threshold has been exceeded		
Remedial action: This alarm is cleared when either the measured memory usage falls below the minimum threshold as aresult of FGW corrective actions or rises above the maximum threshold.. The %CPU column of the top command can be used to check the CPU utilization.Enter the command free to check the memory usage.Free memory specified in the third column must be high compared to the used memory available in second column, for recovering to normal overload.Also, the used buffer cache memory must be low.If the memory usage does not decrease as a result of FGW corrective actions and the alarm is not cleared on its own, terminate some calls and check whether memory utilization comes down and the alarm is clearedIf memory utilization does not come down and overload alarm is still generated, de-register the Small Cells and check whether memory utilization comes down.For further assistance please contact NOKIA customer support.		

Table 28-309 FGW_minimumImsiListThresholdExceeded

Alarm	Attributes	Applicable major release
Name: FGW_minimumImsiListThresholdExceeded (5970) Type: qualityOfServiceAlarm Package: femto.FGW_ minimumImsiListThresholdExceeded Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The number of IMSIs in the ACL lists defined on the SCGW has exceeded the mimimum threshold defined by attribute FGW::minimumIMSIList		
Remedial action: The operator must do a manual clearance.This alarm gets cleared when total number of IMSIs in the ACL lists defined on the BSR Gateway falls below the minimumIMSIList value.		

Table 28-310 FGW_monProcessRestart

Alarm	Attributes	Applicable major release
Name: FGW_monProcessRestart (5971) Type: processingErrorAlarm Package: femto.FGW_monProcessRestart Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW MON forces a process restart.		
Remedial action: NA		

Table 28-311 FGW_nLLInvalidFileFormat

Alarm	Attributes	Applicable major release
Name: FGW_nLLInvalidFileFormat (5972) Type: processingErrorAlarm Package: femto.FGW_nLLInvalidFileFormat Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated if the SCGW detects invalid data in the NLL file		
Remedial action: Log in to the BSR Gateway.Check if the iprange file format is correct in the/opt/natloc/download directory.If the file format is invalid, place the correct IP range file in the /opt/natloc/download directory.This fault is cleared manually from the OAM system.		

Table 28-312 FGW_nLLmultipleFileInDownloadDir

Alarm	Attributes	Applicable major release
Name: FGW_nLLmultipleFileInDownloadDir (5973) Type: processingErrorAlarm Package: femto.FGW_nLLmultipleFileInDownloadDir Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated whenever multiple files have been detected in the NLL download directory on the SCGW		
Remedial action: Log in to the BSR Gateway.Check if multiple ip range files are present in/opt/natloc/download directory.If there are multiple IP range files, the FMG reports to the OAM system, to place a single IP range file in the /opt/natloc/download directory.This fault is cleared manually from the OAM system.		

Table 28-313 FGW_noHeartbeatResponseFromActiveNode

Alarm	Attributes	Applicable major release
Name: FGW_noHeartbeatResponseFromActiveNode (5974) Type: processingErrorAlarm Package: femto.FGW_ noHeartbeatResponseFromActiveNode Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated each time the standby node fails to receive a heartbeat response from the active node within the configured time period,		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active.		

Table 28-314 FGW_percentageNodesRecovered100

Alarm	Attributes	Applicable major release
Name: FGW_percentageNodesRecovered100 (5975) Type: processingErrorAlarm Package: femto.FGW_ percentageNodesRecovered100 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated following a failover in a Redundant Active/Warm Standby configuration, when 100% of small cells have successfully reregistered, compared to the number of standby SCTP associations at the point of failover.		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-315 FGW_percentageNodesRecovered70

Alarm	Attributes	Applicable major release
Name: FGW_percentageNodesRecovered70 (5976) Type: processingErrorAlarm Package: femto.FGW_percentageNodesRecovered70 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated following a failover in a Redundant Active/Warm Standby configuration, when 70% of small cells have successfully reregistered, compared to the number of standby SCTP associations at the point of failover.		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-316 FGW_percentageNodesRecovered80

Alarm	Attributes	Applicable major release
Name: FGW_percentageNodesRecovered80 (5977) Type: processingErrorAlarm Package: femto.FGW_percentageNodesRecovered80 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated following a failover in a Redundant Active/Warm Standby configuration, when 80% of small cells have successfully reregistered, compared to the number of standby SCTP associations at the point of failover.		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-317 FGW_percentageNodesRecovered90

Alarm	Attributes	Applicable major release
Name: FGW_percentageNodesRecovered90 (5978) Type: processingErrorAlarm Package: femto.FGW_percentageNodesRecovered90 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated following a failover in a Redundant Active/Warm Standby configuration, when 90% of small cells have successfully reregistered, compared to the number of standby SCTP associations at the point of failover.		
Remedial action: This alarm is initiated as part of switch-over and there is no explicit corrective procedure for this alarm.Execute the script /opt/scripts/Status.sh to verify whether the current system is active or standby.The alarm is cleared manually from the OAM system once the system status is active.		

Table 28-318 FGW_presenceEventInconsistent

Alarm	Attributes	Applicable major release
Name: FGW_presenceEventInconsistent (5979) Type: integrityViolation Package: femto.FGW_presenceEventInconsistent Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: corruptData	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The Presence Event Indication from the BSR has either the IMSI applicability bit set to 0 and no IMSI included, or the IMSI applicability bit set to 1 and an IMSI included		
Remedial action: Verify the wireshark capture and analyze whether the UE Present Event Indication message sent from the Small Cell has IMSI applicability bit set to 0 and with IMSI included or IMSI applicability bit set to 1 and with no IMSI included. Contact Small Cell support and send a UE Present Event Indication message with any of the following combinations:IMSI applicability bit set to 0 and no IMSI must be includedIMSI applicability bit set to 1 andIMSI must be included		

Table 28-319 FGW_presenceNotActive

Alarm	Attributes	Applicable major release
Name: FGW_presenceNotActive (5980) Type: communicationsAlarm Package: femto.FGW_presenceNotActive Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW receives a BSGAP 'UE Presence Event Indication' from the FemtoBSR when the'activatePresenceAPI' is set to false.		

Table 28-319 FGW_presenceNotActive (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify whether presence is active by using the below commands from BSGCLI command prompt:/opt/bin/BSGCLI. execd FGW<DNNumber>get {activatePresenceAPI};If activatePresenceAPI="False, enablethe PresenceAPI feature using the below commands:/opt/bin/BSGCLI.execd FGW<DNNumber>set {activatePresenceAPI=True};"		

Table 28-320 FGW_resetSuccessful

Alarm	Attributes	Applicable major release
Name: FGW_resetSuccessful (5982) Type: equipmentAlarm Package: femto.FGW_resetSuccessful Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This event is triggered when the system is fully operational after reset		
Remedial action: The system has restarted. No specific operation needed.		

Table 28-321 FGW_rtmConnectionFailure

Alarm	Attributes	Applicable major release
Name: FGW_rtmConnectionFailure (5983) Type: equipmentAlarm Package: femto.FGW_rtmConnectionFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: RTM connection failure		
Remedial action: NA		

Table 28-322 FGW_rTMLinkExceededSeventyPercent

Alarm	Attributes	Applicable major release
Name: FGW_rTMLinkExceededSeventyPercent (5981) Type: communicationsAlarm Package: femto.FGW_ rTMLinkExceededSeventyPercent Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the traffic carried on the link between the Malban unit and the RTM unit exceeds 70 percent of maximum capacity.		
Remedial action: Verify the system configuration.If the problem persists contact Nokia customer support for assistance.		

Table 28-323 FGW_secHardeningProcedureFailure

Alarm	Attributes	Applicable major release
Name: FGW_secHardeningProcedureFailure (11147) Type: securityServiceOrMechanismViolation Package: femto.FGW_secHardeningProcedureFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that a security hardening procedure has failed. Two possible outcomes are implied, (a) the target host may be operationally impaired and/or, (b) the security of the target host may be impaired.		
Remedial action: Root cause analyze the source of the problem and extent of impact. If the host is operationally impacted and is associated with a software upgrade, then the upgrade should be aborted and prior software version restored. Otherwise to address a potentially important security gap, a work around should be explored to cover the security gap and decision on whether or not to accept the software upgrade made on a case basis by a security engineer.If the problem persists, contact Nokia customer support.		

Table 28-324 FGW_shelfManagerConnectionFailure

Alarm	Attributes	Applicable major release
Name: FGW_shelfManagerConnectionFailure (5984) Type: equipmentAlarm Package: femto.FGW_shelfManagerConnectionFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Shelf manager connection failure		
Remedial action: This alarm is cleared automatically by BSR Gateway.This alarm is cleared when the shelfoam is able to communicate with the shelfmanager.This alarm is raised when the active shelfmanagerreboots and gets cleared when the shelfmanager is up.Check if the shelfmanager boards in slot 13 and 14 are operational.If the problem persists, contact Nokia customer support.		

Table 28-325 FGW_shelfManagerConnectionUp

Alarm	Attributes	Applicable major release
Name: FGW_shelfManagerConnectionUp (5985) Type: equipmentAlarm Package: femto.FGW_shelfManagerConnectionUp Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Shelf manager connection up		
Remedial action: No action required		

Table 28-326 FGW_spareAlarmFGWADAC1

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC1 (8478) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC1 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm		

Table 28-327 FGW_spareAlarmFGWADAC2

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC2 (8479) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC2 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm		

Table 28-328 FGW_spareAlarmFGWADAC3

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC3 (8480) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC3 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm		

Table 28-329 FGW_spareAlarmFGWADAC4

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC4 (8481) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC4 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1

Table 28-329 FGW_spareAlarmFGWADAC4 (continued)

Alarm	Attributes	Applicable major release
Description: Spare Alarm 4		
Remedial action: Spare Alarm		

Table 28-330 FGW_spareAlarmFGWADAC5

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC5 (8482) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC5 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm		

Table 28-331 FGW_spareAlarmFGWADAC6

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC6 (8483) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC6 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm		

Table 28-332 FGW_spareAlarmFGWADAC7

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC7 (12991) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC7 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 7		
Remedial action: Spare Alarm		

Table 28-333 FGW_spareAlarmFGWADAC8

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC8 (12992) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC8 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 8		
Remedial action: Spare Alarm		

Table 28-334 FGW_spareAlarmFGWADAC9

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADAC9 (12993) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADAC9 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC20.1
Description: Spare Alarm 9		
Remedial action: Spare Alarm		

Table 28-335 FGW_spareAlarmFGWADMC1

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC1 (8484) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC1 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm		

Table 28-336 FGW_spareAlarmFGWADMC2

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC2 (8485) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC2 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		

Table 28-336 FGW_spareAlarmFGWADMC2 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Spare Alarm		

Table 28-337 FGW_spareAlarmFGWADMC3

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC3 (8486) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC3 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm		

Table 28-338 FGW_spareAlarmFGWADMC4

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC4 (8487) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC4 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm		

Table 28-339 FGW_spareAlarmFGWADMC5

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC5 (8488) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC5 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm		

Table 28-340 FGW_spareAlarmFGWADMC6

Alarm	Attributes	Applicable major release
Name: FGW_spareAlarmFGWADMC6 (8489) Type: processingErrorAlarm Package: femto.FGW_spareAlarmFGWADMC6 Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm		

Table 28-341 FGW_sshKeySharingNotCorrect

Alarm	Attributes	Applicable major release
Name: FGW_sshKeySharingNotCorrect (9018) Type: equipmentAlarm Package: femto.FGW_sshKeySharingNotCorrect Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proceduralError	Release: • SC17.2 • SC19.1 • SC20.1
Description: SSH Key is not shared properly between the nodes		
Remedial action: Synchronize SSH keys between nodes		

Table 28-342 FGW_strmgrRedirectPDUDecodeFailed

Alarm	Attributes	Applicable major release
Name: FGW_strmgrRedirectPDUDecodeFailed (5986) Type: processingErrorAlarm Package: femto.FGW_ strmgrRedirectPDUDecodeFailed Raised on class: femto.FGW	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated whenever the SCGW has detected a failure to decode a Redirect PDU for Femto to Femto Handover		
Remedial action: When the incoming message PDU size is greater than the control PDU size, then the alarm raised.If the message for Redirect does not have a Begin Indication flag, then this alarm is raised.Check at the Small Cell side for the root cause and send another Small Cell to Small Cell redirect request.This fault is cleared manually from the OAM system when hand over happens successfully.		

Table 28-343 FGW_switchOver

Alarm	Attributes	Applicable major release
Name: FGW_switchOver (5987) Type: processingErrorAlarm Package: femto.FGW_switchOver Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when switchover of SCGW Node happens at Central router		
Remedial action: This alarm is cleared when switchover successfully happens.This is verified by checking the system state after switchover.This alarm is manually cleared from the OAM system.If the problem persists, contact Nokia customer support.		

Table 28-344 FGW_sysHardResetInitiated

Alarm	Attributes	Applicable major release
Name: FGW_sysHardResetInitiated (5988) Type: equipmentAlarm Package: femto.FGW_sysHardResetInitiated Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is triggered when hard reset is initiated in SCGW when it automatically resets due to system failure		
Remedial action: NA		

Table 28-345 FGW_sysSoftResetInitiated

Alarm	Attributes	Applicable major release
Name: FGW_sysSoftResetInitiated (5989) Type: equipmentAlarm Package: femto.FGW_sysSoftResetInitiated Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is triggered when soft reset is initiated in SCGW when it resets due to system failure		
Remedial action: NA		

Table 28-346 FGW_unstableSCTPAssociation

Alarm	Attributes	Applicable major release
Name: FGW_unstableSCTPAssociation (8490) Type: communicationsAlarm Package: femto.FGW_unstableSCTPAssociation Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is raised if the SCTP association to the Access Point has been unstable with many short term interruptions		
Remedial action: Investigate the stability of the back haul links between the Access Point and SCGW		

Table 28-347 FGW_violationBufferOverflow

Alarm	Attributes	Applicable major release
Name: FGW_violationBufferOverflow (5990) Type: qualityOfServiceAlarm Package: femto.FGW_violationBufferOverflow Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when the SCGW buffer used to store aclViolation, bsrIntegrity and bsrIdClash alarms is exceeded.		
Remedial action: This alarm is raised when the violation buffer exceeds the limit.The violation buffer size is set from the BSGCLI.The fault is cleared manually from the OAM system.		

Table 28-348 FGW_vlanCreationFailure

Alarm	Attributes	Applicable major release
Name: FGW_vlanCreationFailure (5991) Type: equipmentAlarm Package: femto.FGW_vlanCreationFailure Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: VLAN creation failure		
Remedial action: Execute the command ifconfig to verify the VLAN creation.Clear the alarm manually from the OAM system if the VLAN creation is successful.		

Table 28-349 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 28-350 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 28-351 GenericNatProxy_genericNATproxyServiceFailure

Alarm	Attributes	Applicable major release
Name: GenericNatProxy_ genericNATproxyServiceFailure (5999) Type: communicationsAlarm Package: femto.GenericNatProxy_ genericNATproxyServiceFailure Raised on class: femto.GenericNatProxy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unavailable	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-351 GenericNatProxy_genericNATproxyServiceFailure (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised if the DNS resolution of an FQDN configured in GenericNatProxy::serverAddress fails. The alarm is cleared when the DNS resolution of the FQDN succeeds		
Remedial action: Check the configured FQDN in GenericNatProxy::serverAddress is validCheck that the FQDN is registered in DNS.		

Table 28-352 HardDiskSlot_diskUsageNearingCapacity

Alarm	Attributes	Applicable major release
Name: HardDiskSlot_diskUsageNearingCapacity (6001) Type: equipmentAlarm Package: femto.HardDiskSlot_ diskUsageNearingCapacity Raised on class: femto.HardDiskSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the disk usage has exceeded seventy percent of available capacity. The alarm is automatically cleared whenever disk usage is reduced below thirty percent of available capacity.		
Remedial action: Cleanup unnecessary backups,files to bring down disk usage.		

Table 28-353 HardDisk_diskUsageNearingCapacity

Alarm	Attributes	Applicable major release
Name: HardDisk_diskUsageNearingCapacity (6002) Type: equipmentAlarm Package: femto.HardDisk_diskUsageNearingCapacity Raised on class: femto.HardDisk	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised whenever the disk usage has exceeded seventy percent of available capacity. The alarm is automatically cleared whenever disk usage is reduced below thirty percent of available capacity.		
Remedial action: Cleanup unnecessary backups,files to bring down disk usage.		

Table 28-354 HeNBMasterCP_rangeOfStreamsFromHeNBNotSupported

Alarm	Attributes	Applicable major release
Name: HeNBMasterCP_ rangeOfStreamsFromHeNBNotSupported (6003) Type: communicationsAlarm Package: femto.HeNBMasterCP_ rangeOfStreamsFromHeNBNotSupported Raised on class: femto.HeNBMasterCP	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1

Table 28-354 HeNBMasterCP_rangeOfStreamsFromHeNBNotSupported (continued)

Alarm	Attributes	Applicable major release
Description: This fault indicates a mismatch between the number of input & output streams configured on the gateway and the number of input & output streams received from HeNB during SCTP INIT negotiation HeNB ID shall be mentioned in the alarm description so that operator can identify the HeNBThis alarm can be used for Small Cells Monitoring (Service Monitoring) feature		
Remedial action: Check the configuration for the number of input and output steams supported by the HeNB.The number of input and output streams are expected to be equal and to have indetifiers in the range [0..511]. So HeNB configuration needs to be corrected for input and output SCTP streams.This alarm should be manually cleared by the OAM system's user.If the problem persists, contact Nokia customer support.		

Table 28-355 HeNBMasterCP_spareAlarmHeNBMasterCP1

Alarm	Attributes	Applicable major release
Name: HeNBMasterCP_spareAlarmHeNBMasterCP1 (12398) Type: equipmentAlarm Package: femto.HeNBMasterCP_ spareAlarmHeNBMasterCP1 Raised on class: femto.HeNBMasterCP	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-356 HeNBMasterCP_spareAlarmHeNBMasterCP2

Alarm	Attributes	Applicable major release
Name: HeNBMasterCP_spareAlarmHeNBMasterCP2 (12399) Type: equipmentAlarm Package: femto.HeNBMasterCP_ spareAlarmHeNBMasterCP2 Raised on class: femto.HeNBMasterCP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-357 HeNBMasterCP_spareAlarmHeNBMasterCP3

Alarm	Attributes	Applicable major release
Name: HeNBMasterCP_spareAlarmHeNBMasterCP3 (12400) Type: equipmentAlarm Package: femto.HeNBMasterCP_ spareAlarmHeNBMasterCP3 Raised on class: femto.HeNBMasterCP	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 1		

Table 28-358 HeNBMasterUP_noUserPlaneMapping

Alarm	Attributes	Applicable major release
Name: HeNBMasterUP_noUserPlaneMapping (12401) Type: processingErrorAlarm Package: femto.HeNBMasterUP_ noUserPlaneMapping Raised on class: femto.HeNBMasterUP	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the SCGW receives a user plane packet which gets discarded due to there being no associated binding in the UserPlane mapping table		
Remedial action: NA		

Table 28-359 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 28-360 IPSP_aspDown

Alarm	Attributes	Applicable major release
Name: IPSP_aspDown (6004) Type: communicationsAlarm Package: femto.IPSP_aspDown Raised on class: femto.IPSP	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Notification to inform the application that SCGW's IPSP instance for CS and PS connections is now down		
Remedial action: Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM to restore the link.On completion of successful handshake, ASPUP messages are exchanged between the BSR Gateway and Core Network.This fault is automatically cleared by the clear alarm IPSP_ASPDOWNCLEARANCE.Run BSGConsole.exe. Use the below command in active FGW to check the destination point code status.bsg_get_destination_status<dpc>Check the link connectivity.Investigate the fault at the core network.If the problem persists, contact Nokia customer support		

Table 28-361 IPSP_aspInactive

Alarm	Attributes	Applicable major release
Name: IPSP_aspInactive (6005) Type: communicationsAlarm Package: femto.IPSP_aspInactive Raised on class: femto.IPSP	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Notification to inform the application that the SCGW's IPSP instance has become inactive		
Remedial action: Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM to restore the link.This fault is automatically cleared by the clear alarmIPSP_ASPINACTIVECLEARANCE.Run BSGConsole.exe. Use the command in active FGW to check the destination point code status:bsg_get_destination_status<dpc>Check the link connectivity.Investigate the fault at the core network.If the problem persists, contact Nokia customer support		

Table 28-362 IPSP_ICM_EVENT_BND_FAIL

Alarm	Attributes	Applicable major release
Name: IPSP_ICM_EVENT_BND_FAIL (6006) Type: communicationsAlarm Package: femto.IPSP_ICM_EVENT_BND_FAIL Raised on class: femto.IPSP	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Generated if the bind procedure with the lower layer fails. The bind procedure can fail either due to the absence of bind confirm, or if there is a negative bind confirm from the lower layer.		

Table 28-362 IPSP_ICM_EVENT_BND_FAIL (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is cleared automatically by the clear alarm IPSP_ICM_EVENT_BND_OK.Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM to make the M3UA lower SAP bind with SCTP successful.Perform stopbsg and switchover if the alarm is not cleared for a long time.If the problem persists, contact Nokia customer support.		

Table 28-363 IPSP_IIT_EVENT_ESTABLISH_FAIL

Alarm	Attributes	Applicable major release
Name: IPSP_IIT_EVENT_ESTABLISH_FAIL (6007) Type: communicationsAlarm Package: femto.IPSP_IIT_EVENT_ESTABLISH_FAIL Raised on class: femto.IPSP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Generated if association establishment fails. If it is an association to a remote SG, the SG ID is given by s.sgId. If it is an association to a remote ASP, the ASP ID is given by s.aspId.		
Remedial action: The alarm is cleared automatically by the Clear Alarm IPSP_IIT_EVENT_ESTABLISH_OK.		

Table 28-364 IPSP_IIT_EVENT_SCT_COMM_DOWN

Alarm	Attributes	Applicable major release
Name: IPSP_IIT_EVENT_SCT_COMM_DOWN (6008) Type: communicationsAlarm Package: femto.IPSP_IIT_EVENT_SCT_COMM_DOWN Raised on class: femto.IPSP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Generated when an the SCTP service provider indicates that an association has lost communications		
Remedial action: NA		

Table 28-365 IPSP_IIT_EVENT_TERM_IND

Alarm	Attributes	Applicable major release
Name: IPSP_IIT_EVENT_TERM_IND (6009) Type: communicationsAlarm Package: femto.IPSP_IIT_EVENT_TERM_IND Raised on class: femto.IPSP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Generated when a termination indication is received from the SCTP service provider		

Table 28-365 IPSP_IIT_EVENT_TERM_IND (continued)

Alarm	Attributes	Applicable major release
Remedial action: When the association establishment procedure is successful for the Iu Interface, and ESTABLISH_OK event is received, the alarm is cleared automatically by the Clear Alarm IPSP_IIT_EVENT_ESTABLISH_OK.Perform stopbsg and switchover if the association establishment procedure is not successful for a long time.		

Table 28-366 IuBC_cellBroadcastCenterFailure

Alarm	Attributes	Applicable major release
Name: IuBC_cellBroadcastCenterFailure (6019) Type: communicationsAlarm Package: femto.IuBC_cellBroadcastCenterFailure Raised on class: femto.IuBC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Communication with the Cell Broadcast Center has been lost.		
Remedial action: Check that the IP addresses entered for the cell broadcast center in ipAddressCellBroadcastPrimary and ipAddressCellBroadcastSecondary are correct.Check the connectivity to the Cell Broadcast Center.		

Table 28-367 IuBC_cellBroadcastOverload

Alarm	Attributes	Applicable major release
Name: IuBC_cellBroadcastOverload (6020) Type: qualityOfServiceAlarm Package: femto.IuBC_cellBroadcastOverload Raised on class: femto.IuBC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm shall be raised when the threshold has been reached for the number of concurrent inprogress SABP procedures handled by the gateway		
Remedial action: Wait until the existing SABP procedures have completed before sending additional requests.		

Table 28-368 IuCSMGW_remoteMTP3Unreachable

Alarm	Attributes	Applicable major release
Name: IuCSMGW_remoteMTP3Unreachable (6021) Type: communicationsAlarm Package: femto.IuCSMGW_remoteMTP3Unreachable Raised on class: femto.IuCSMGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-368 IuCSMGW_remoteMTP3Unreachable (continued)

Alarm	Attributes	Applicable major release
Description: All routes to reach the MTP3 at this destination (i.e. Media Gateway) have failed.		
Remedial action: Check the status of the remote MTP3 on the remote device		

Table 28-369 IuCSMGW_remoteMTP3UserUnavailable

Alarm	Attributes	Applicable major release
Name: IuCSMGW_remoteMTP3UserUnavailable (6022) Type: communicationsAlarm Package: femto.IuCSMGW_ remoteMTP3UserUnavailable Raised on class: femto.IuCSMGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The user of the MTP3 (i.e. ALCAP/STC.1) on the peer node is not available for service		
Remedial action: Check the status of the remote MTP3 on the remote device		

Table 28-370 IuCSUserplaneVCL_aConfigFailure

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_aConfigFailure (6024) Type: processingErrorAlarm Package: femto.IuCSUserplaneVCL_aConfigFailure Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The userplane configuration is failed in ALCAP. To recover from this failure, degrow this IuCSUserplaneVCL and regrow again.		
Remedial action: NA		

Table 28-371 IuCSUserplaneVCL_aEndToEndConnectionFailure

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_ aEndToEndConnectionFailure (6025) Type: communicationsAlarm Package: femto.IuCSUserplaneVCL_ aEndToEndConnectionFailure Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-371 IuCSUserplaneVCL_aEndToEndConnectionFailure (continued)

Alarm	Attributes	Applicable major release
Description: Multiple CS calls that were having bearers on this userplane has faced end to end bearer failures. This will be cleared upon a successful call establishment and teardown.		
Remedial action: NA		

Table 28-372 IuCSUserplaneVCL_aLocallyBlockedForAdminLock

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_ aLocallyBlockedForAdminLock (6026) Type: processingErrorAlarm Package: femto.IuCSUserplaneVCL_ aLocallyBlockedForAdminLock Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The userplane is locally blocked due to local admin Lock action. This will be cleared after the admin state changes to unlocked.		
Remedial action: NA		

Table 28-373 IuCSUserplaneVCL_aLocallyBlockedForBearerFailures

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_ aLocallyBlockedForBearerFailures (6027) Type: processingErrorAlarm Package: femto.IuCSUserplaneVCL_ aLocallyBlockedForBearerFailures Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The userplane is locally blocked due to multiple call failures resulted due to end-to-end bearer issues. This will be cleared either after one successful call is released or upon the ALCAP trying to unblock upon a expiry		
Remedial action: NA		

Table 28-374 IuCSUserplaneVCL_aLocallyBlockedForUnblockCfm

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_ aLocallyBlockedForUnblockCfm (6028) Type: communicationsAlarm Package: femto.IuCSUserplaneVCL_ aLocallyBlockedForUnblockCfm Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-374 IuCSUserplaneVCL_aLocallyBlockedForUnblockCfm (continued)

Alarm	Attributes	Applicable major release
Description: The userplane is locally blocked and the unblock procedure is under progress with the peer node and wating for Unblock Confirm. This will be cleared after successful reception of Unblock Confirm from peer.		
Remedial action: NA		

Table 28-375 IuCSUserplaneVCL_aRemotelyBlocked

Alarm	Attributes	Applicable major release
Name: IuCSUserplaneVCL_aRemotelyBlocked (6029) Type: communicationsAlarm Package: femto.IuCSUserplaneVCL_ aRemotelyBlocked Raised on class: femto.IuCSUserplaneVCL	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteNodeTransmissionError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The userplane is remotely blocked by the peer node. This will be cleared after the remote successfully unblocks the userplane.		
Remedial action: NA		

Table 28-376 IuCS_aspInactive

Alarm	Attributes	Applicable major release
Name: IuCS_aspInactive (6030) Type: communicationsAlarm Package: femto.IuCS_aspInactive Raised on class: femto.IuCS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Notification to inform the application that the FGW's IPSP instance has become inactive		
Remedial action: NA		

Table 28-377 IuCS_destinationMSCNotReachable

Alarm	Attributes	Applicable major release
Name: IuCS_destinationMSCNotReachable (6031) Type: communicationsAlarm Package: femto.IuCS_destinationMSCNotReachable Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-377 IuCS_destinationMSCNotReachable (continued)

Alarm	Attributes	Applicable major release
Description: This fault is generated when 3G-MSC is not reachable from the SCGW		
Remedial action: Check the vlan by pinging the ipaddress and also the association existence using the command Cat /proc/net/sctp/assoc.Use wireshark to capture trace and BSR Gateway logs and check if SSP is in prohibited state or whether AS is in inactive state.Check whether the PC is unavailable or route is unavailableCheck the configuration settings on the BSR Gateway and the Core Network and correct the configuration if necessary.Retry the communication between the Core Network and the BSR Gateway.This alarm is cleared after successful handshake with the Core Network.It can be verified in Wireshark capture and also by executing calls through that interface.		

Table 28-378 IuCS_emergencyCallfailed

Alarm	Attributes	Applicable major release
Name: IuCS_emergencyCallfailed (6032) Type: communicationsAlarm Package: femto.IuCS_emergencyCallfailed Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW could not handle Emergency Call		
Remedial action: Check the connectivity between BSR Gateway and MSC.Check whether BSR Gateway socket towards MSC is opened.Check for the ERROR/FATAL log statements related to this issue.This alarm is manually cleared from the OAM system.		

Table 28-379 IuCS_failedToSendPAGINGToBSR

Alarm	Attributes	Applicable major release
Name: IuCS_failedToSendPAGINGToBSR (6033) Type: communicationsAlarm Package: femto.IuCS_failedToSendPAGINGToBSR Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send PAGING message to BSR		
Remedial action: Check for the log statement Failed to send PAGING, BSR Instin Log_FMG.log file. This prints the association ID of the Small Cell for which the paging message failed.Check for the Small Cells registeredin the BSR Gateway console using the command bsg_get_bsr_registrations.If there is no Small Cell registered with the BSR Gateway, retry the scenario after registering the Small Cells with the BSR Gateway.Perform paging from the Core Network and check whether any new alarm is generated.This fault is manually cleared at the OAM system.		

Table 28-380 IuCS_failedToSendRelocationRequestMsgToDestBSR

Alarm	Attributes	Applicable major release
Name: IuCS_ failedToSendRelocationRequestMsgToDestBSR (6034) Type: communicationsAlarm Package: femto.IuCS_ failedToSendRelocationRequestMsgToDestBSR Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW could not send Relocation Request message to the BSR		
Remedial action: Check whether the Small Cell is registered with the BSR Gateway.Check whether there are FATAL/ERROR logs in Log_FMG.log with respect to this issue.Use the above mentioned information to isolate the issue at Small Cell or BSR Gateway end.This fault is manually cleared from the OAM system. Clear the alarm if the next relocation request message sent from BSR Gateway reaches the destination Small Cell.		

Table 28-381 IuCS_iuCsInterfaceInactive

Alarm	Attributes	Applicable major release
Name: IuCS_iuCsInterfaceInactive (6035) Type: communicationsAlarm Package: femto.IuCS_iuCsInterfaceInactive Raised on class: femto.IuCS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unavailable	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The IuCS interface has become inactive as the number of dropped inbound massages has been exceeded. This indicates a potential locking of the IuCS interface or fault at the Core Network.		
Remedial action: Check if the administrative state of IuCS interface is set to locked. If locked then unlock the IuCS interface.Run BSGConsole.exe. Use the command in active FGW to check the destination point code status:bsg_get_destination_status<dpc> Check the link connectivity.Investigate the fault at the SGSN end.Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM torestore the link.The alarm is cleared automatically by the clear alarmIUCS_IUCSINTERFACEINACTIVECLEARANCE, if CN responds for furtherconnection requests from the FGW.If the problem persists, contact Nokia customer support		

Table 28-382 IuCS_noBSRConnectedToBSG

Alarm	Attributes	Applicable major release
Name: IuCS_noBSRConnectedToBSG (6036) Type: communicationsAlarm Package: femto.IuCS_noBSRConnectedToBSG Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to forward CL messages to BSR since no BSRs are connected		

Table 28-382 IuCS_noBSRConnectedToBSG (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check for the Small Cells registered in the BSR Gateway Console using the command bsg_get_bsr_registrations. Register the Small Cell and retry the CS call.If there is no Small Cell registered, then register the Small Cells with the BSR Gateway and retry the scenario again.This fault is manually cleared from the OAM system.		

Table 28-383 IuCS_noBSRInReceivedLAC

Alarm	Attributes	Applicable major release
Name: IuCS_noBSRInReceivedLAC (6037) Type: communicationsAlarm Package: femto.IuCS_noBSRInReceivedLAC Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives paging message from a MSC for which no BSR is registered		
Remedial action: Check for the FATAL/ERROR log messages in Log_FMG.log for the relevant error messages.If the Small Cell is not registered, register the Small Cell.Issue the same paging message again.Clear the alarm manually.		

Table 28-384 IuCS_receivedMTP3PauseSPInaccessible

Alarm	Attributes	Applicable major release
Name: IuCS_receivedMTP3PauseSPInaccessible (6038) Type: communicationsAlarm Package: femto.IuCS_ receivedMTP3PauseSPInaccessible Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCCP stack receives MTP3-Pause due to deactivation of link indicating remote point inaccessible.		
Remedial action: This alarm is automatically cleared by theBSGwhen the remote point code of MSCis accessible and in allowed state.		

Table 28-385 IuCS_receivedPauseForMSC

Alarm	Attributes	Applicable major release
Name: IuCS_receivedPauseForMSC (6039) Type: communicationsAlarm Package: femto.IuCS_receivedPauseForMSC Raised on class: femto.IuCS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-385 IuCS_receivedPauseForMSC (continued)

Alarm	Attributes	Applicable major release
Description: This fault is generated when SCGW is not able to access MSC due to failure of connection towards MSC		
Remedial action: Check the point codes configured for the particular Iu interface at the the BSR Gateway as well as in the core network.Make necessary changes if the configuration is incorrect.Run BSGConsole.exe. Use the command in active FGW to check the destination point code status:bsg_get_destination_status<dpc> Check the link connectivity.Investigate the fault at the MSC end.Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM to restore the link.This fault is cleared automatically when the destination point code for a CS domaininterface is in available state, that is, when destination point code/route available message is received.The clearance alarm is IUCS_RECEIVEDPAUSEFORMSCCLEARANCE.This can be verified by Wireshark capture and also by executing calls.If the problem persists, contact Nokia customer support.		

Table 28-386 IuCS_remoteMTP3Unreachable

Alarm	Attributes	Applicable major release
Name: IuCS_remoteMTP3Unreachable (6040) Type: communicationsAlarm Package: femto.IuCS_remoteMTP3Unreachable Raised on class: femto.IuCS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: All routes to reach the MTP3 at this destination (i.e. MSC server) have failed.		
Remedial action: Check the availability status of the remote systemIf the problem persists, contact Nokia customer support		

Table 28-387 IuCS_remoteMTP3UserUnavailable

Alarm	Attributes	Applicable major release
Name: IuCS_remoteMTP3UserUnavailable (6041) Type: communicationsAlarm Package: femto.IuCS_remoteMTP3UserUnavailable Raised on class: femto.IuCS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The user of the MTP3 (i.e. SCCP) on the peer node is not available for service		
Remedial action: Check the availability status of the remote system		

Table 28-388 IuCS_remoteSubsystemOutOfService

Alarm	Attributes	Applicable major release
Name: IuCS_remoteSubsystemOutOfService (6042) Type: processingErrorAlarm Package: femto.IuCS_remoteSubsystemOutOfService Raised on class: femto.IuCS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The remote subsystem has gone out of service		
Remedial action: Check the status of the remote system		

Table 28-389 IuPC_destinationSASNotReachable

Alarm	Attributes	Applicable major release
Name: IuPC_destinationSASNotReachable (8492) Type: communicationsAlarm Package: femto.IuPC_destinationSASNotReachable Raised on class: femto.IuPC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when operator SAS is not reachable from the SCGW		
Remedial action: Check the vlan by pinging the ipaddress and also the association existence using the command Cat /proc/net/sctp/assoc. Use wireshark to capture trace and SCGW logs and check if SSP is in prohibited state or whether AS is in inactive state.Check whether the PC is unavailable or route is unavailable Check the configuration settings on the SCGW and the Core Network and correct the configuration if necessary. Retry the communication between the Core Network and the SCGW. This alarm is cleared after successful handshake with the Core Network. It can be verified in Wireshark capture and also by executing calls through that interface.		

Table 28-390 IuPC_positionInitiationGlobalTransactionIdExhausted

Alarm	Attributes	Applicable major release
Name: IuPC_ positionInitiationGlobalTransactionIdExhausted (8493) Type: qualityOfServiceAlarm Package: femto.IuPC_ positionInitiationGlobalTransactionIdExhausted Raised on class: femto.IuPC	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: The pool of Global Transaction Ids for use with PCAP Position Initiation Request procedures is 95% exhausted		
Remedial action: Alarm occurs due to high rate of RANAP Location Report Control procedures for UEs in Small Cell coverage. Consider reducing frequency of these procedures. Consider use of RNC centric location procedures rather than SAS centric . Automatically cleared when transaction id usage recovers to less than 90%.		

Table 28-391 IuPS_aspInactive

Alarm	Attributes	Applicable major release
Name: IuPS_aspInactive (6044) Type: communicationsAlarm Package: femto.IuPS_aspInactive Raised on class: femto.IuPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Notification to inform the application that the FGW's IPSP instance has become inactive		
Remedial action: NA		

Table 28-392 IuPS_destinationSGSNNotReachable

Alarm	Attributes	Applicable major release
Name: IuPS_destinationSGSNNotReachable (6045) Type: communicationsAlarm Package: femto.IuPS_destinationSGSNNotReachable Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SGSN is not reachable from the SCGW		
Remedial action: Check the vlan by pinging the ipaddressand also the association existence using the commandCat /proc/net/sctp/assoc.Use wireshark capture trace and FGW logs and check if SSP is in prohibited state or whether AS is in inactive state.Check whether PC is unavailable or route is unavailable.Check the configuration settings at BSR Gateway and the CN and correct the configuration if necessary.Retry communication between the CN and the BSR Gateway.When CN establishes communication with the BSR Gateway successfully, this alarm is cleared after successful handshake with core network.		

Table 28-393 IuPS_failedToSendPAGINGToBSR

Alarm	Attributes	Applicable major release
Name: IuPS_failedToSendPAGINGToBSR (6046) Type: communicationsAlarm Package: femto.IuPS_failedToSendPAGINGToBSR Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send PAGING message to BSR		
Remedial action: Check for the log statement Failed to send PAGING, BSR Instin Log_FMG.log file. This prints the association ID of the Small Cell for which the paging message failed.Check for the Small Cells registeredin the BSR Gateway console using the command bsg_get_bsr_registrations.If there is no Small Cell registered with the BSR Gateway, retry the scenario after registering the Small Cells with the BSR Gateway.Perform paging from the Core Network and check whether any new alarm is generated.This fault is manually cleared at the OAM system.		

Table 28-394 IuPS_failedToSendRANAPResetToBSR

Alarm	Attributes	Applicable major release
Name: IuPS_failedToSendRANAPResetToBSR (6047) Type: communicationsAlarm Package: femto.IuPS_ failedToSendRANAPResetToBSR Raised on class: femto.IuPS	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send RANAP RESET message to BSR		
Remedial action: Check the status of the interface to the BSR.		

Table 28-395 IuPS_failedToSendRelocationRequestMsgToDestBSR

Alarm	Attributes	Applicable major release
Name: IuPS_ failedToSendRelocationRequestMsgToDestBSR (6048) Type: communicationsAlarm Package: femto.IuPS_ failedToSendRelocationRequestMsgToDestBSR Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW could not send Relocation Request message to the BSR		
Remedial action: Check whether the Small Cell is registered with the BSR Gateway.Check whether there are FATAL/ERROR logs in Log_FMG.log with respect to this issue.Use the above mentioned information to isolate the issue at Small Cell or BSR Gateway end.This fault is manually cleared from the OAM system. Clear the alarm if the next relocation request message sent from BSR Gateway reaches the destination Small Cell.		

Table 28-396 IuPS_failedToSendResetResourceToBSR

Alarm	Attributes	Applicable major release
Name: IuPS_failedToSendResetResourceToBSR (6049) Type: communicationsAlarm Package: femto.IuPS_ failedToSendResetResourceToBSR Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to send Reset Resource message to BSR		
Remedial action: Check the status of the interface to the BSR.		

Table 28-397 IuPS_gtpEchoFailure

Alarm	Attributes	Applicable major release
Name: IuPS_gtpEchoFailure (6050) Type: communicationsAlarm Package: femto.IuPS_gtpEchoFailure Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: No response to repetitive GTP-U Echo Requests from BPG to SGSN for a particular active connection.		
Remedial action: The SGSN machine must be up and running.Check for proper cable connections between the SGSN and the BTG. Verify whether the response is properly sent and received.Initiate PS call between Small Cell and SGSN. The GTP echo request is raised automatically from the BTG machine to the SGSN machine.Verify the connection is established with Small Cell and BTG through BTGConsole. Run BTGConsole application and enter btg_get_bpg_table. The rule is present for the corresponding Small Cell and SGSN.When a GTP Echo response is received from SGSN then the alarm is auto cleared by BTG.Verify the alarm is raised or not from the BTG log file /opt/log/BTG/Log_BTG.log using the pattern IUPS_GTPECHOFAILURE ALARM clearance raised.		

Table 28-398 IuPS_iuPsInterfaceInactive

Alarm	Attributes	Applicable major release
Name: IuPS_iuPsInterfaceInactive (6051) Type: communicationsAlarm Package: femto.IuPS_iuPsInterfaceInactive Raised on class: femto.IuPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unavailable	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The IuPS interface has become inactive as the number of dropped inbound massages has been exceeded. This indicates a potential locking of the IuPS interface or fault at the Core Network.		
Remedial action: Check if the administrative state of IuPS interface is set to locked. If locked thenunlock the IuPS interface.Run BSGConsole.exe. Use the command bsg_get_destination_status<dpc> in active FGW to check the destination point code status.Check the link connectivity.Investigate the fault at the SGSN end.Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM torestore the link.The alarm is cleared automatically by the clear alarmIUPS_IUPSINTERFACEINACTIVECLEARANCE, if CN responds for furtherconnection requests from the FGW.If the problem persists, contact Nokia customer support.		

Table 28-399 IuPS_noBSRConnectedToBSG

Alarm	Attributes	Applicable major release
Name: IuPS_noBSRConnectedToBSG (6052) Type: communicationsAlarm Package: femto.IuPS_noBSRConnectedToBSG Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW fails to forward CL messages to BSR since no BSRs are connected		

Table 28-399 IuPS_noBSRConnectedToBSG (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check for the Small Cells registered in the BSR Gateway Console using the command bsg_get_bsr_registrations. Register the Small Cell and retry the CS call.If there is no Small Cell registered, then register the Small Cells with the BSR Gateway and retry the scenario again.This fault is manually cleared from the OAM system.		

Table 28-400 IuPS_noBSRInReceivedRAC

Alarm	Attributes	Applicable major release
Name: IuPS_noBSRInReceivedRAC (6053) Type: communicationsAlarm Package: femto.IuPS_noBSRInReceivedRAC Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCGW receives a paging message for an RAC and no BSR is registered for that RAC		
Remedial action: Check the fatal/error log messages in Log_FMG.logfor the relevant error messages.If the Small Cell is not registered, then register the same.Issue the same paging message again.Clear the alarm manually.		

Table 28-401 IuPS_receivedMTP3PauseSPInaccessible

Alarm	Attributes	Applicable major release
Name: IuPS_receivedMTP3PauseSPInaccessible (6054) Type: communicationsAlarm Package: femto.IuPS_ receivedMTP3PauseSPInaccessible Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when SCCP stack receives MTP3-Pause due to deactivation of link indicating remote point inaccessible.		
Remedial action: This alarm is automatically cleared by theBSGwhen the remote point code of MSCis accessible and in allowed state.		

Table 28-402 IuPS_receivedPauseForSGSN

Alarm	Attributes	Applicable major release
Name: IuPS_receivedPauseForSGSN (6055) Type: communicationsAlarm Package: femto.IuPS_receivedPauseForSGSN Raised on class: femto.IuPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-402 IuPS_receivedPauseForSGSN (continued)

Alarm	Attributes	Applicable major release
Description: This fault is generated when SCGW is not able to access SGSN due to connection failure towards SGSN		
Remedial action: Check the point codes status at BSR Gateway and SGSN and the configuration settings at BSR Gateway and SGSN.Run BSGConsole.exe. Use the command bsg_get_destination_status<dpc> in active FGW to check the destination point code status.Check the link connectivity.Investigate the fault at the SGSN end.Perform SCTPAssociation administrative state lock/unlock from FGW CLI/SAM to restore the link.This fault is cleared automatically when the destination point code for a PS domain interface is in available state (when destination point code/Route available message is received).The clearance alarm is IUPS_ RECEIVEDPAUSEFORSGSNCLEARANCE.This can be verified by Wireshark capture and also by executing calls.If the problem persists, contact Nokia customer support.		

Table 28-403 IuPS_remoteMTP3Unreachable

Alarm	Attributes	Applicable major release
Name: IuPS_remoteMTP3Unreachable (6056) Type: communicationsAlarm Package: femto.IuPS_remoteMTP3Unreachable Raised on class: femto.IuPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: All routes to reach the MTP3 at this destination (i.e. SGSN) have failed.		
Remedial action: Check the availability status of the remote systemIf the problem persists, contact Nokia customer support		

Table 28-404 IuPS_remoteMTP3UserUnavailable

Alarm	Attributes	Applicable major release
Name: IuPS_remoteMTP3UserUnavailable (6057) Type: communicationsAlarm Package: femto.IuPS_remoteMTP3UserUnavailable Raised on class: femto.IuPS	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmitFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The user of the MTP3 (i.e. SCCP) on the peer node is not available for service		
Remedial action: Check the status of the remote system		

Table 28-405 IuPS_remoteSubsystemOutOfService

Alarm	Attributes	Applicable major release
Name: IuPS_remoteSubsystemOutOfService (6058) Type: processingErrorAlarm Package: femto.IuPS_remoteSubsystemOutOfService Raised on class: femto.IuPS	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The remote subsystem has gone out of service		
Remedial action: Check the availability status of the remote systemIf the problem persists, contact Nokia customer support		

Table 28-406 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 28-407 LegalReq_legalReqFileDeliveryFailure

Alarm	Attributes	Applicable major release
Name: LegalReq_legalReqFileDeliveryFailure (6090) Type: communicationsAlarm Package: femto.LegalReq_legalReqFileDeliveryFailure Raised on class: femto.LegalReq	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: transmissionError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW fails to deliver a legal requisition data file to the collection server.		
Remedial action: Verify whether LR server is reachable by pinging to the ip address of the LRServer.Verify whether public key authentication has been enabled between BSR Gateway and LR Server (when manual SFTP from BSR Gateway to LR Server is tried, user should not be prompted for password).Verify the directory permissions on the LRServer is root:root and the permission is 755. This fault will be cleared automatically when BSR Gateway succeeds in sending a previously failed legal req file.		

Table 28-408 LegalReq_legalReqFileDeliveryFailureclearance

Alarm	Attributes	Applicable major release
Name: LegalReq_ legalReqFileDeliveryFailureclearance (6091) Type: processingErrorAlarm Package: femto.LegalReq_ legalReqFileDeliveryFailureclearance Raised on class: femto.LegalReq	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is generated when the FGW succeeds in sending a previously failed legal req file.		
Remedial action: NA		

Table 28-409 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 28-410 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		

Table 28-410 LinkDown (equipment) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 28-411 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 28-412 MeNBMasterCP_spareAlarmMeNBMasterCP1

Alarm	Attributes	Applicable major release
Name: MeNBMasterCP_spareAlarmMeNBMasterCP1 (12998) Type: equipmentAlarm Package: femto.MeNBMasterCP_ spareAlarmMeNBMasterCP1 Raised on class: femto.MeNBMasterCP	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-413 MeNBMasterCP_spareAlarmMeNBMasterCP2

Alarm	Attributes	Applicable major release
Name: MeNBMasterCP_spareAlarmMeNBMasterCP2 (12999) Type: equipmentAlarm Package: femto.MeNBMasterCP_ spareAlarmMeNBMasterCP2 Raised on class: femto.MeNBMasterCP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1

Table 28-413 MeNBMasterCP_spareAlarmMeNBMasterCP2 (continued)

Alarm	Attributes	Applicable major release
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-414 MeNBMasterCP_spareAlarmMeNBMasterCP3

Alarm	Attributes	Applicable major release
Name: MeNBMasterCP_spareAlarmMeNBMasterCP3 (13000) Type: equipmentAlarm Package: femto.MeNBMasterCP_ spareAlarmMeNBMasterCP3 Raised on class: femto.MeNBMasterCP	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-415 MMERegion_invalidTacRegion

Alarm	Attributes	Applicable major release
Name: MMERegion_invalidTacRegion (6095) Type: communicationsAlarm Package: femto.MMERegion_invalidTacRegion Raised on class: femto.MMERegion	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is raised when operators configures a region with a TAC that is already used by an existing region		
Remedial action: Correct the region's configuration in the appropriate MMERegion object		

Table 28-416 MMERegion_s1InterfaceFailure

Alarm	Attributes	Applicable major release
Name: MMERegion_s1InterfaceFailure (6096) Type: communicationsAlarm Package: femto.MMERegion_s1InterfaceFailure Raised on class: femto.MMERegion	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: S1 Interface towards all the MME's in this MMERegion are down.		
Remedial action: Check the status of the MMEs.Check the communication path to the MME.This fault is automatically cleared by the clear alarmMMEREGION_S1INTERFACEFAILURECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-417 MME_rangeOfStreamsFromMMENotSupported

Alarm	Attributes	Applicable major release
Name: MME_rangeOfStreamsFromMMENotSupported (6097) Type: communicationsAlarm Package: femto.MME_ rangeOfStreamsFromMMENotSupported Raised on class: femto.MME	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that an uneqal number of input and output streams have been received from the MME or a S1AP message with an invalid stream id has been received		
Remedial action: MME configuration needs to be corrected for input and output SCTP streams.This alarm should be manually cleared by the OAM system's user..If the problem persists, contact Nokia customer support.		

Table 28-418 MME_s1InterfaceDown

Alarm	Attributes	Applicable major release
Name: MME_s1InterfaceDown (6098) Type: communicationsAlarm Package: femto.MME_s1InterfaceDown Raised on class: femto.MME	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the S1 Setup procedure fails towards towards the MME (i.e. No S1 Setup Response after several retries or reception of S1 Setup Failure response). This indicates the s1Interface down and no other procedure can be performed towards the MME.		
Remedial action: Check the status of the MME.Check the communication path to the MME.This fault is automatically cleared by the clear alarmMME_S1INTERFACEDOWNCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-419 MME_s1InterfaceInactive

Alarm	Attributes	Applicable major release
Name: MME_s1InterfaceInactive (6099) Type: communicationsAlarm Package: femto.MME_s1InterfaceInactive Raised on class: femto.MME	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that S1 link between SCGW and MME has been locked through an OAM action. This alarm gets cleared when S1 link is unlocked		
Remedial action: Perform unlock operation for MME on the OAM system GUI.This fault is automatically cleared by the clear alarmMME_S1INTERFACEINACTIVECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-420 MME_s1SCTPAssociationDown

Alarm	Attributes	Applicable major release
Name: MME_s1SCTPAssociationDown (6100) Type: communicationsAlarm Package: femto.MME_s1SCTPAssociationDown Raised on class: femto.MME	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates SCTP assoication failure between SCGW and MME.		
Remedial action: Check the status of the MME.Check the communication path to the MME.This fault is automatically cleared by the clear alarmMME_S1SCTPASSOCIATIONDOWNCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-421 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 28-422 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 28-422 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 28-423 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 28-424 NextHopHeartBeat_fgwActiveSRLinkDown

Alarm	Attributes	Applicable major release
Name: NextHopHeartBeat_fgwActiveSRLinkDown (6151) Type: communicationsAlarm Package: femto.NextHopHeartBeat_ fgwActiveSRLinkDown Raised on class: femto.NextHopHeartBeat	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that SCGW Active node cannot reach one of the SRs connected to it. This alarm shall be raised for each SR failure		
Remedial action: Check the connection between the gateway and the service router for the active SR link.If the problem persists, contact Nokia customer support.		

Table 28-425 NextHopHeartBeat_fgwStandbySRLinkDown

Alarm	Attributes	Applicable major release
Name: NextHopHeartBeat_fgwStandbySRLinkDown (6152) Type: communicationsAlarm Package: femto.NextHopHeartBeat_ fgwStandbySRLinkDown Raised on class: femto.NextHopHeartBeat	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that SCGW Standby node cannot reach one of the SRs connected to it. This alarm shall be raised for each SR failure		
Remedial action: Check the connection between the gateway and the service router for the standby SR linkIf the problem persists, contact Nokia customer support.		

Table 28-426 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 28-427 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 28-427 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 28-428 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 28-429 OAM_223

Alarm	Attributes	Applicable major release
Name: OAM_223 (6164) Type: communicationsAlarm Package: femto.OAM_223 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • 4.0.0
Description: Some of the SCGW PM files are missing. Please check the SCGW logs for reasons on why the PM files are missing.		
Remedial action: Check the communication link between PM Server and FileServer. This notification may be required by Global Product Support for debugging purposes		

Table 28-430 OverloadedCard

Alarm	Attributes	Applicable major release
Name: OverloadedCard (2941) Type: cardAlarm Package: equipment.OverloadedCard Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: overloadedCard	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when an ATCA card becomes overloaded.		
Raising condition: (('Overload State' EQUAL 'Critical') OR ('Overload State' EQUAL 'Resource Critical'))		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Investigate /opt/tpa/logs/RACServer.log on the CSB to determine cause of system overload.		

Table 28-431 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 28-432 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		

Table 28-432 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 28-433 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 28-434 PCIEthernetCard_cardFailure

Alarm	Attributes	Applicable major release
Name: PCIEthernetCard_cardFailure (6165) Type: equipmentAlarm Package: femto.PCIEthernetCard_cardFailure Raised on class: femto.PCIEthernetCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when PCI Ethernet card failure occurs		
Remedial action: Check whether the Ethernet card to be installed in the X4250 system, is recommended by SUN.Check whether the PCIe Ethernet card is inserted in the appropriate slot.Check whether there are any alignment issues while installing the Ethernet card.Rectify the problems and reboot the system.Connect the cable to the card and check whether the LED is blinking, indicating flow of traffic.After receiving EthernetPort_cardFailure clearance alarm, the operator must do a manual clearance.		

Table 28-435 PCIEthernetPort_cardFailure

Alarm	Attributes	Applicable major release
Name: PCIEthernetPort_cardFailure (6166) Type: equipmentAlarm Package: femto.PCIEthernetPort_cardFailure Raised on class: femto.PCIEthernetPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when a PCI Ethernet Port failure occurs		
Remedial action: Check whether the Ethernet card to be installed in the X4250 system, is recommended by SUN.Check whether the PCIe Ethernet card is inserted in the appropriate slot.Check whether there are any alignment issues while installing the Ethernet card.Rectify the problems and reboot the system.Connect the cable to the card and check whether the LED is blinking, indicating flow of traffic.After receiving EthernetPort_cardFailure clearance alarm, the operator must do a manual clearance.		

Table 28-436 PCIEthernetPort_interfaceActive

Alarm	Attributes	Applicable major release
Name: PCIEthernetPort_interfaceActive (6167) Type: communicationsAlarm Package: femto.PCIEthernetPort_interfaceActive Raised on class: femto.PCIEthernetPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the PCI Ethernet Port interface is up		
Remedial action: The operator must do a manual clearance.		

Table 28-437 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		

Table 28-437 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 28-438 PhysicalInterfaceB_vLANInterfaceDown

Alarm	Attributes	Applicable major release
Name: PhysicalInterfaceB_vLANInterfaceDown (6170) Type: communicationsAlarm Package: femto.PhysicalInterfaceB_ vLANInterfaceDown Raised on class: femto.PhysicalInterfaceB	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that VLAN is not reachable and it is not active.		
Remedial action: Ensure that the VLAN is properly configured on all the nexthops switches and routers.The fault is automatically cleared byPHYSICALINTERFACEB_VLANINTERFACEDOWNCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-439 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 28-440 PowerModule_voltageALocalFailure

Alarm	Attributes	Applicable major release
Name: PowerModule_voltageALocalFailure (6171) Type: environmentalAlarm Package: femto.PowerModule_voltageALocalFailure Raised on class: femto.SCATCAPowerModule	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when the 48V Voltage Failure happens in the power supply A of the local Shelf.		
Remedial action: See the nodal documentation for more information.		

Table 28-441 PowerModule_voltageARemoteFailure

Alarm	Attributes	Applicable major release
Name: PowerModule_voltageARemoteFailure (6172) Type: environmentalAlarm Package: femto.PowerModule_voltageARemoteFailure Raised on class: femto.SCATCAPowerModule	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when the 48V Voltage Failure happens in the power supply A of the remote Shelf.		
Remedial action: See the nodal documentation for more information.		

Table 28-442 PowerModule_voltageBLocalFailure

Alarm	Attributes	Applicable major release
Name: PowerModule_voltageBLocalFailure (6173) Type: environmentalAlarm Package: femto.PowerModule_voltageBLocalFailure Raised on class: femto.SCATCAPowerModule	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when the 48V Voltage Failure happens in the power supply B of the local Shelf.		
Remedial action: See the nodal documentation for more information.		

Table 28-443 PowerModule_voltageBRemoteFailure

Alarm	Attributes	Applicable major release
Name: PowerModule_voltageBRemoteFailure (6174) Type: environmentalAlarm Package: femto.PowerModule_voltageBRemoteFailure Raised on class: femto.SCATCAPowerModule	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • 4.0.0
Description: This Alarm is raised when the 48V Voltage Failure happens in the power supply B of the remote Shelf.		
Remedial action: See the nodal documentation for more information.		

Table 28-444 PowerSupplySlot_presenceDetectedAssert

Alarm	Attributes	Applicable major release
Name: PowerSupplySlot_presenceDetectedAssert (6175) Type: physicalViolation Package: femto.PowerSupplySlot_ presenceDetectedAssert Raised on class: femto.PowerSupplySlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence detected assert		
Remedial action: Check if the power supply slot in the system is faulty.Reboot the system after rectifying the issue.After receiving PowerSupplySlot_presenceDetectedAssert alarm operator must do manual clearance.		

Table 28-445 PowerSupplySlot_presenceDetectedDeassert

Alarm	Attributes	Applicable major release
Name: PowerSupplySlot_presenceDetectedDeassert (6176) Type: physicalViolation Package: femto.PowerSupplySlot_ presenceDetectedDeassert Raised on class: femto.PowerSupplySlot	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Presence detected de-assert		
Remedial action: The alarm is cleared manually from the OAM system.		

Table 28-446 PowerSupplySlot_pwrSupFailuerDeassert

Alarm	Attributes	Applicable major release
Name: PowerSupplySlot_pwrSupFailuerDeassert (6177) Type: equipmentAlarm Package: femto.PowerSupplySlot_ pwrSupFailuerDeassert Raised on class: femto.PowerSupplySlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: powerProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Predictive failure assert		
Remedial action: Manual switch to redundant system recommended to address the power supply problem.		

Table 28-447 PowerSupplySlot_pwrSupFailureAssert

Alarm	Attributes	Applicable major release
Name: PowerSupplySlot_pwrSupFailureAssert (6178) Type: equipmentAlarm Package: femto.PowerSupplySlot_ pwrSupFailureAssert Raised on class: femto.PowerSupplySlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Power supply failure detected assert		
Remedial action: Check for voltage fluctuations in the system as a result of power supply failure.Check if there are issues within the power regulator in the system and in the service processor card.Reboot the system after rectifying the above issues.After receiving PowerSupplySlot_pwrSupFailuerDeassert alarm operator must do a manual clearance.		

Table 28-448 PowerSupplySlot_pwrSupInputLost

Alarm	Attributes	Applicable major release
Name: PowerSupplySlot_pwrSupInputLost (6179) Type: equipmentAlarm Package: femto.PowerSupplySlot_pwrSupInputLost Raised on class: femto.PowerSupplySlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: powerProblem	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Power supply input lost assert		
Remedial action: Check for the power supply input, to see if there are any fluctuations.Verify whether the power supply unit within the system is in functional order.Reboot the system after rectifying the problems.After restoring operator must do manual clearance.		

Table 28-449 Presence_presenceServerFailure

Alarm	Attributes	Applicable major release
Name: Presence_presenceServerFailure (6180) Type: communicationsAlarm Package: femto.Presence_presenceServerFailure Raised on class: femto.PresenceServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Communication with a Presence server has been lost.		
Remedial action: Obtain the presence server ID, from the last index of the OID, printed in the alarm raised at the OAM system.In SSH session, execute the following commands, to check for IPAddress of presence server, from BSGCLI:/opt/bin/BSGCLI.execd FGW:<DNNumber>/BSG:<DNNumber>/Presence:<PresenceServerID >;get {presenceserver};presenceserver="<IPAddress_of_ Presence_Server>To ping the presence server, execute:Ping <IPAddress_of_Presence_Server>If the destination is reachable then presence server is active.If the destination is not reachable then check for the availability of presence server.The alarm is automatically detected and cleared by the BSR Gateway, once the presence server establishes communication with the Gateway."		

Table 28-450 Presence_publishRespBadEvent

Alarm	Attributes	Applicable major release
Name: Presence_publishRespBadEvent (6181) Type: communicationsAlarm Package: femto.Presence_publishRespBadEvent Raised on class: femto.PresenceServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW receives a 489 (Bad Event) response in return to a SIP PUBLISH		
Remedial action: Using wireshark capture, check whether the publish message framed by the BSR Gateway holds the SipIfMatch header.If SipIfMatch header is present in the publish message sent from the BSR Gateway, using logs check the presence server not holding the entry. Contact PS support to solve this issue.If SipIfMatch header is not present in publish message sent from the BSR Gateway, contact BSR Gateway support for an updated BSR Gateway package.Clear the alarm manually from the the OAM system once the issue is fixed.		

Table 28-451 Presence_publishRespInvalidReq

Alarm	Attributes	Applicable major release
Name: Presence_publishRespInvalidReq (6182) Type: communicationsAlarm Package: femto.Presence_publishRespInvalidReq Raised on class: femto.PresenceServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW receives a 400 (Invalid Request) response in return to a SIP PUBLISH		
Remedial action: When the incoming message PDU size is greater than the control PDU size, then the alarm raised.If the message for Redirect does not have a Begin Indication flag, then this alarm is raised.Check at the Small Cell side for the root cause and send another Small Cell to Small Cell redirect request.This fault is cleared manually from the OAM system when hand over happens successfully.		

Table 28-452 Presence_publishRespNotFound

Alarm	Attributes	Applicable major release
Name: Presence_publishRespNotFound (6183) Type: communicationsAlarm Package: femto.Presence_publishRespNotFound Raised on class: femto.PresenceServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW receives a 404 (Not Found) response in return to a SIP PUBLISH		

Table 28-452 Presence_publishRespNotFound (continued)

Alarm	Attributes	Applicable major release
Remedial action: Using wireshark capture, check whether the publish message framed by the BSR Gateway holds the SipIfMatch header.If SipIfMatch header is present in the publish message sent from the BSR Gateway, using logs check the presence server not holding the entry. Contact PS support to solve this issue.If SipIfMatch header is not present in publish message sent from the BSR Gateway, contact BSR Gateway support for an updated BSR Gateway package.Clear the alarm manually from the OAM system once the issue is fixed.		

Table 28-453 Presence_publishRespTimeOut

Alarm	Attributes	Applicable major release
Name: Presence_publishRespTimeOut (6184) Type: communicationsAlarm Package: femto.Presence_publishRespTimeOut Raised on class: femto.PresenceServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated if the SCGW received no respone after SIP PUBLISHretransmissions are exhausted		
Remedial action: Check the format of the SIP publish message sent from the BSR Gateway and from the PS server logs for any issues in the publish message.If the BSR Gateway is not sending the message in the format expected by PS, contact BSR Gateway support to solve the issue.Clear the alarm manually from the OAM system once the issue is fixed.		

Table 28-454 Presence_publishRespUnsupMediaType

Alarm	Attributes	Applicable major release
Name: Presence_publishRespUnsupMediaType (6185) Type: communicationsAlarm Package: femto.Presence_publishRespUnsupMediaType Raised on class: femto.PresenceServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCGW receives a 415 (Unsupported Media Type) response in return to a SIP PUBLISH		
Remedial action: Using wireshark captures, check whether the publish message sent by the BSR Gateway holds the Content-Type header.If exist, check whether the Content-Type sent by the BSR Gateway is accepted by presence server using PS logs. Contact support team if the Content-Type is supported by the PS, but it will throw 415 error.Contact BSR Gateway support if the Content-Type is not supported by the PS.Clear the alarm manually from the OAM system once the issue is fixed.		

Table 28-455 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 28-456 ProcessMonitor_processRestart

Alarm	Attributes	Applicable major release
Name: ProcessMonitor_processRestart (6186) Type: processingErrorAlarm Package: femto.ProcessMonitor_processRestart Raised on class: femto.ProcessMonitor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: operationalCondition	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when this process has had an unexpected restart.		
Remedial action: This alarm is automatically cleared by the BSR Gateway after a successful restart.		

Table 28-457 ProcessMonitor_processRestartThreshold

Alarm	Attributes	Applicable major release
Name: ProcessMonitor_processRestartThreshold (6187) Type: processingErrorAlarm Package: femto.ProcessMonitor_ processRestartThreshold Raised on class: femto.ProcessMonitor	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the number of restarts counted for this process has exceeded the threshold defined by attribute restartThreshold		
Remedial action: Verify whether the restart count of the process is below the threshold.This alarm is cleared manually from the OAM system if the count is below the threshold.If the problem persists, contact Nokia customer support		

Table 28-458 PsRegion_invalidSuperLacOverlap

Alarm	Attributes	Applicable major release
Name: PsRegion_invalidSuperLacOverlap (6188) Type: integrityViolation Package: femto.PsRegion_invalidSuperLacOverlap Raised on class: femto.PsRegion	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Incorrect configuration for superLAC values which have different superLACs for overlapping regions.		
Remedial action: Check the BSG configuration OAM_Preconfig.xml file and make sure the PSRegion and superLAC configurations are correct.The operator must do a manual clearance.		

Table 28-459 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 28-460 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		

Table 28-460 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 28-461 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 28-462 RTM_rtmMP3_3V

Alarm	Attributes	Applicable major release
Name: RTM_rtmMP3_3V (6191) Type: equipmentAlarm Package: femto.RTM_rtmMP3_3V Raised on class: femto.SCATCARTM	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to RTM 3.3V monitoring from the carrier.		
Remedial action: See the nodal documentation for more information.		

Table 28-463 RTM_rtmPower12V

Alarm	Attributes	Applicable major release
Name: RTM_rtmPower12V (6192) Type: equipmentAlarm Package: femto.RTM_rtmPower12V Raised on class: femto.SCATCARTM	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to RTM 12V monitoring from the carrier.		

Table 28-463 RTM_rtmPower12V (continued)

Alarm	Attributes	Applicable major release
Remedial action: See the nodal documentation for more information.		

Table 28-464 RTM_rtmPowerCurrent

Alarm	Attributes	Applicable major release
Name: RTM_rtmPowerCurrent (6193) Type: equipmentAlarm Package: femto.RTM_rtmPowerCurrent Raised on class: femto.SCATCARTM	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to RTM current monitoring from the carrier.		
Remedial action: See the nodal documentation for more information.		

Table 28-465 RTM_rtmPowerPGD

Alarm	Attributes	Applicable major release
Name: RTM_rtmPowerPGD (6194) Type: equipmentAlarm Package: femto.RTM_rtmPowerPGD Raised on class: femto.SCATCARTM	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • 4.0.0
Description: This Alarm is raised when failure happens to Power supply status,from the RTM point of view.		
Remedial action: See the nodal documentation for more information.		

Table 28-466 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 28-467 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 28-468 SCTPAssociation_remoteSCTPCommDown

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_remoteSCTPCommDown (11163) Type: communicationsAlarm Package: femto.SCTPAssociation_ remoteSCTPCommDown Raised on class: femto.SCTPAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: Generated when an the SCTP service provider indicates that an association has lost communications with the remote node		
Remedial action: When the association establishment procedure with remote node is successful, the alarm is cleared automatically.Perform stopbsg and switchover if the association establishment procedure is not successful for a long time.		

Table 28-469 SCTPAssociation_sCTPCantStart

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_sCTPCantStart (6206) Type: communicationsAlarm Package: femto.SCTPAssociation_sCTPCantStart Raised on class: femto.SCTPAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when a peer did not respond to an association setup attempt.		

Table 28-469 SCTPAssociation_sCTPCantStart (continued)

Alarm	Attributes	Applicable major release
Remedial action: When the SCTP handshake is done for an Iu Interface, and SCT_COMM_UP event is received.This can be verified by executing calls with corresponding the Core Network.Perform stopbsg and switch-over if the association establishment procedure is not successful for a long time.		

Table 28-470 SCTPAssociation_sCTPcommunicationLost

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_sCTPcommunicationLost (6208) Type: communicationsAlarm Package: femto.SCTPAssociation_ sCTPcommunicationLost Raised on class: femto.SCTPAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the SCTP association is down (which means all redundant paths are failed)		
Remedial action: When the core network is reachable and SCTP handshake is done for an Iu Interface, SCT_COMM_UP event is received.Perform stopbsg and switchover if the association establishment procedure is not successful for a long time.		

Table 28-471 SCTPAssociation_sCTPpathError

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_sCTPpathError (8500) Type: communicationsAlarm Package: femto.SCTPAssociation_sCTPpathError Raised on class: femto.SCTPAssociation	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when there is a fault in the current path of SCTP association.		
Remedial action: No action. SCTP association continues to work with alternate path.		

Table 28-472 SCTPAssociation_sCTPPeerAddressChange

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_sCTPPeerAddressChange (6207) Type: communicationsAlarm Package: femto.SCTPAssociation_ sCTPPeerAddressChange Raised on class: femto.SCTPAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This notification informs the application that one of the peer's addresses has experienced a change of state		

Table 28-472 SCTPAssociation_sCTPPeerAddressChange (continued)

Alarm	Attributes	Applicable major release
Remedial action: This fault needs to be cleared manually.Successful establishment of core network communication with the BSG after modifications will clear the alarm.Perform stopbsg and switchover if the association establishment procedure is not successful for a long time.		

Table 28-473 SCTPAssociation_sCTPPeerRestart

Alarm	Attributes	Applicable major release
Name: SCTPAssociation_sCTPPeerRestart (11164) Type: communicationsAlarm Package: femto.SCTPAssociation_sCTPPeerRestart Raised on class: femto.SCTPAssociation	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when a RESTART notification is received on a SCTP association from remote peer node.		
Remedial action: No remedial action needed.		

Table 28-474 ServerHardware_chassisIntrusionAssert

Alarm	Attributes	Applicable major release
Name: ServerHardware_chassisIntrusionAssert (6221) Type: physicalViolation Package: femto.ServerHardware_ chassisIntrusionAssert Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Physical Security. Chassis intrusion assert		
Remedial action: Check if the chassis has been opened or if there is any misalignment of the chassis cover.Secure the chassis cover properly and make sure its closed properly.After getting ServerHardware_chassisIntrusionDeassert alarm, the operator must do a manual clearance.		

Table 28-475 ServerHardware_chassisIntrusionDeassert

Alarm	Attributes	Applicable major release
Name: ServerHardware_chassisIntrusionDeassert (6222) Type: physicalViolation Package: femto.ServerHardware_ chassisIntrusionDeassert Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Physical Security. Chassis intrusion de-assert		

Table 28-475 ServerHardware_chassisIntrusionDeassert (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action needed.Informational alarm which indicates that alarm condition is now cleared		

Table 28-476 ServerHardware_dnsServerDown

Alarm	Attributes	Applicable major release
Name: ServerHardware_dnsServerDown (6223) Type: processingErrorAlarm Package: femto.ServerHardware_dnsServerDown Raised on class: femto.ServerHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the DNS server within FGW hardware is out of service.		
Remedial action: NA		

Table 28-477 ServerHardware_dskRedDegraded

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedDegraded (6224) Type: equipmentAlarm Package: femto.ServerHardware_dskRedDegraded Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Disk redundancy degraded assert. Redundancy still exists, but at a less than full level. This will not normally be used in the SCGW.		
Remedial action: Check if any of the disk in the logical volume has gone down.Check if the disk is accessible via software.Check BIOS configuration and make sure the RAID configuration is properly done.Replace the disk if necessary.Check with HW support and rectify the issue.Check the functionality of all disks after correction.User must clear this alarm after receiving the alarm serverHardware_ dskRedRegained.		

Table 28-478 ServerHardware_dskRedDegradedFromFull

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedDegradedFromFull (6225) Type: equipmentAlarm Package: femto.ServerHardware_ dskRedDegradedFromFull Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-478 ServerHardware_dskRedDegradedFromFull (continued)

Alarm	Attributes	Applicable major release
Description: Redundant degrade from fully redundant assert. Unit has lost some disk redundant resource(s) but is still in a redundant state. Entered by a transition from Fully Redundant condition. This will not normally be used in the SCGW.		
Remedial action: Check if any of the disk in the logical volume has gone down.Check if the disk is accessible via software.Check BIOS configuration and make sure the RAID configuration is properly done.Replace the disk if necessary.Check with HW support and rectify the issue.Check the functionality of all disks after correction.User must clear this alarm after receiving the alarm serverHardware_ dskRedRegained.		

Table 28-479 ServerHardware_dskRedInsufficientResource

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedInsufficientResource (6226) Type: equipmentAlarm Package: femto.ServerHardware_ dskRedInsufficientResource Raised on class: femto.ServerHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Non redundant insufficient resources assert. Unit is non-redundant and has insufficient power supply resources to maintain normal operation.		
Remedial action: Check the functionality of all disks and check power slots, power cables and power regulators.User can clear this alarm after receiving the alarm serverHardware_dskRedRegained.		

Table 28-480 ServerHardware_dskRedLost

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedLost (6227) Type: equipmentAlarm Package: femto.ServerHardware_dskRedLost Raised on class: femto.ServerHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Disk redundancy lost assert. Entered any non-redundant state, including Non-redundant: Insufficient Resources		
Remedial action: Check if any of the disk in the logical volume has gone down.Check if the disk is accessible via software.Check BIOS configuration and make sure the RAID configuration is properly done.Replace the disk if necessary.Check with HW support and rectify the issue.Check the functionality of all disks after correction.User must clear this alarm after receiving the alarm serverHardware_ dskRedRegained.		

Table 28-481 ServerHardware_dskRedLostFunctioning

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedLostFunctioning (6228) Type: equipmentAlarm Package: femto.ServerHardware_ dskRedLostFunctioning Raised on class: femto.ServerHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Non redundant sufficient resources . Disk redundancy has been lost but unit is functioning with minimum resources needed for 'normal' operation. Entered from Redundancy Degraded or Fully Redundant.		
Remedial action: Check if any of the disk in the logical volume has gone down.Check if the disk is accessible via software.Check BIOS configuration and make sure the RAID configuration is properly done.Replace the disk if necessary.Check with HW support and rectify the issue.Check the functionality of all disks after correction.User must clear this alarm after receiving the alarm serverHardware_ dskRedRegained.		

Table 28-482 ServerHardware_dskRedMinimumResource

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedMinimumResource (6229) Type: equipmentAlarm Package: femto.ServerHardware_ dskRedMinimumResource Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Non redundant sufficient from insufficient resources assert. Unit has regained minimum disk resources needed for 'normal' operation. Entered from Non-redundant:Insufficient Resources		
Remedial action: Check if any of the disk in the logical volume has gone down.Check if the disk is accessible via software.Check BIOS configuration and make sure the RAID configuration is properly done.Replace the disk if necessary.Check with HW support and rectify the issue.Check the functionality of all disks after correction.User must clear this alarm after receiving the alarm serverHardware_ dskRedRegained.		

Table 28-483 ServerHardware_dskRedNotFullyRedundant

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedNotFullyRedundant (6230) Type: equipmentAlarm Package: femto.ServerHardware_ dskRedNotFullyRedundant Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Redundant degraded from non redundant assert. Unit has regained some disk resource(s) and is redundant but not fully redundant. Entered from Non-redundant:Sufficient Resources or Non-redundant:Insufficient Resources. This will not normally be used in the SCGW.		

Table 28-483 ServerHardware_dskRedNotFullyRedundant (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operator must do a manual clearance, after receiving the alarm serverHardware_dskRedRegained..		

Table 28-484 ServerHardware_dskRedRegained

Alarm	Attributes	Applicable major release
Name: ServerHardware_dskRedRegained (6231) Type: equipmentAlarm Package: femto.ServerHardware_dskRedRegained Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Fully redundant assert. Indicates that full disk redundancy has been regained.		
Remedial action: No action needed.Informational alarm which indicates that disk redundancy is now restored.		

Table 28-485 ServerHardware_lAANLostDeassert

Alarm	Attributes	Applicable major release
Name: ServerHardware_lAANLostDeassert (6232) Type: physicalViolation Package: femto.ServerHardware_lAANLostDeassert Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LAN leash lost de-assert		
Remedial action: No action needed.Informational alarm which indicates that the condition is now cleared.		

Table 28-486 ServerHardware_lANLostAssert

Alarm	Attributes	Applicable major release
Name: ServerHardware_lANLostAssert (6233) Type: physicalViolation Package: femto.ServerHardware_lANLostAssert Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: LAN leash lost assert. System is unplugged from LAN		

Table 28-486 ServerHardware_lANLostAssert (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check whether the Ethernet cables are properly connected to the card and the ports are blinking.Check for Ethernet card issues in the box.Check whether the ports at the Service Router are configured properly.Reboot the system and start up the Ethernet interface, and assign IP addresses.Check if the ping to the service router is working fine.After receiving the ServerHardware_ lAANLostDeassert alarm, the operator must do a manual clearance.		

Table 28-487 ServerHardware_platformSecOutOfBandPswd

Alarm	Attributes	Applicable major release
Name: ServerHardware_platformSecOutOfBandPswd (6234) Type: securityServiceOrMechanismViolation Package: femto.ServerHardware_ platformSecOutOfBandPswd Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Platform Security Violation. Out-of-band access password violation assert		
Remedial action: Investigate the security voilation and proceed.		

Table 28-488 ServerHardware_platformSecViolationAttempt

Alarm	Attributes	Applicable major release
Name: ServerHardware_platformSecViolationAttempt (6235) Type: securityServiceOrMechanismViolation Package: femto.ServerHardware_ platformSecViolationAttempt Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: intrusionDetection	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Platform Security Violation. Secure mode violation attempt assert		
Remedial action: Investigate the security voilation and proceed.		

Table 28-489 ServerHardware_pwrRedDegraded

Alarm	Attributes	Applicable major release
Name: ServerHardware_pwrRedDegraded (6236) Type: equipmentAlarm Package: femto.ServerHardware_pwrRedDegraded Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0

Table 28-489 ServerHardware_pwrRedDegraded (continued)

Alarm	Attributes	Applicable major release
Description: Power supple redundancy degraded assert. Redundancy still exists, but at a less than full level. For example, a system has four fans, and can tolerate the failure of two of them, and presently one has failed.		
Remedial action: Check for any cooling device failure.Perform system reboot after rectifying the cooling device.After receiving the ServerHardware_pwrRedRegained alarm, operator must do manual clearance.		

Table 28-490 ServerHardware_pwrRedInsufficientResource

Alarm	Attributes	Applicable major release
Name: ServerHardware_pwrRedInsufficientResource (6237) Type: equipmentAlarm Package: femto.ServerHardware_ pwrRedInsufficientResource Raised on class: femto.ServerHardware	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Non redundant insufficient resources assert. Unit is non-redundant and has insufficient power supply resources to maintain normal operation.		
Remedial action: Check if there is sufficient power supply to the server.Check if the power supply card within the CG server is faulty.Rectify the power supply input to the CG server or the power supply card.Reboot the system.After receiving ServerHardware_ pwrRedRegained alarm, operator must do a manual clearance.		

Table 28-491 ServerHardware_pwrRedLost

Alarm	Attributes	Applicable major release
Name: ServerHardware_pwrRedLost (6238) Type: equipmentAlarm Package: femto.ServerHardware_pwrRedLost Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Power supply redundancy lost assert. Entered any non-redundant state, including Non-redundant: Insufficient Resources		
Remedial action: Check and restore the failed power supply.Power restore must be checked by the LED which glows in the server in the front end near the power on button. When the LED indicates green color, it determines successful power restoration.Power restore can also be checked using the ipmitoolcommand.ipmitool -I open chassis statusOn receiving ServerHardware_pwrRedRegained alarm, operator must do a manual clearance.		

Table 28-492 ServerHardware_pwrRedMinimumResource

Alarm	Attributes	Applicable major release
Name: ServerHardware_pwrRedMinimumResource (6239) Type: equipmentAlarm Package: femto.ServerHardware_ pwrRedMinimumResource Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Non redundant sufficient from insufficient resources assert. Unit has regained minimum power supply resources needed for 'normal' operation. Entered from Non-redundant:Insufficient Resources		
Remedial action: Check if the power supply card is functioning.Reboot the system after rectifying the power supply card.After receiving ServerHardware_pwrRedRegained alarm, operator must do a manual clearance.		

Table 28-493 ServerHardware_pwrRedRegained

Alarm	Attributes	Applicable major release
Name: ServerHardware_pwrRedRegained (6240) Type: equipmentAlarm Package: femto.ServerHardware_pwrRedRegained Raised on class: femto.ServerHardware	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Fully redundant assert. Indicates that full power supply redundancy has been regained.		
Remedial action: Check for any cooling device failure.Perform system reboot after rectifying the cooling device.After receiving the ServerHardware_pwrRedRegained alarm, operator must do manual clearance.		

Table 28-494 ServerHardware_sntpServerDown

Alarm	Attributes	Applicable major release
Name: ServerHardware_sntpServerDown (6241) Type: processingErrorAlarm Package: femto.ServerHardware_sntpServerDown Raised on class: femto.ServerHardware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This fault is generated when the ToD server within FGW hardware is out of service		
Remedial action: NA		

Table 28-495 SgNBCommon_gNBDataFileEntryError

Alarm	Attributes	Applicable major release
Name: SgNBCommon_gNBDataFileEntryError (13002) Type: processingErrorAlarm Package: femto.SgNBCommon_ gNBDataFileEntryError Raised on class: femto.SgNBCommon	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC20.1
Description: This fault is generated when the X2Aggregator has detected one or more erroneous entries in the SgNB CSV Data file e.g. duplicate or multiple SgNB IDs details for a given macro eNB/IP address.		
Remedial action: Make the required corrections for duplicate/multiple SgNB ID entries in the CSV file and trigger the File Download again using ActSgNBData action.		

Table 28-496 SgNBCommon_gNBDataFileInvalid

Alarm	Attributes	Applicable major release
Name: SgNBCommon_gNBDataFileInvalid (13003) Type: processingErrorAlarm Package: femto.SgNBCommon_gNBDataFileInvalid Raised on class: femto.SgNBCommon	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC20.1
Description: This fault is generated when the X2Aggregator has detected that the format of the 5G macro SgNB Data File is corrupt or has an invalid format		
Remedial action: Verify that the CSV file downloaded from the OAM system is syntactically correct.Make the required corrections in the CSV file and trigger the File Download again using ActSgNBData action.		

Table 28-497 SgNBCommon_gNBDataFileMissing

Alarm	Attributes	Applicable major release
Name: SgNBCommon_gNBDataFileMissing (13004) Type: processingErrorAlarm Package: femto.SgNBCommon_gNBDataFileMissing Raised on class: femto.SgNBCommon	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileError	Release: • SC20.1
Description: This fault is generated when the X2Aggregator has detected that the 5G SgNB Macro CSV file gNBMacroData.csv is not present in /opt/MacroSgNBData/ directory.		
Remedial action: Re-trigger the 5G gNB CSV file transfer action from SAM usingActSgNBData action.Check that the gNBMacroData. csv file is is successfully downloaded in /opt/MacroSgNBData/ directory.		

Table 28-498 SgNBCommon_gNBX2AssociationDown

Alarm	Attributes	Applicable major release
Name: SgNBCommon_gNBX2AssociationDown (13005) Type: communicationsAlarm Package: femto.SgNBCommon_ gNBX2AssociationDown Raised on class: femto.SgNBCommon	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • SC20.1
Description: This fault indicates abnormal SCTP assoication failure between X2Aggregator and SgNB.		
Remedial action: Check the status of the SgNB.Check the communication path to the SgNB.This fault is automatically cleared by the clear alarm SgNB_S1SCTPASSOCIATIONDOWNCLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-499 SgNBCommon_spareAlarmSgNBCommon1

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon1 (13006) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon1 Raised on class: femto.SgNBCommon	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-500 SgNBCommon_spareAlarmSgNBCommon2

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon2 (13007) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon2 Raised on class: femto.SgNBCommon	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-501 SgNBCommon_spareAlarmSgNBCommon3

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon3 (13008) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon3 Raised on class: femto.SgNBCommon	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-502 SgNBCommon_spareAlarmSgNBCommon4

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon4 (13009) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon4 Raised on class: femto.SgNBCommon	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm 4		

Table 28-503 SgNBCommon_spareAlarmSgNBCommon5

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon5 (13010) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon5 Raised on class: femto.SgNBCommon	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm 5		

Table 28-504 SgNBCommon_spareAlarmSgNBCommon6

Alarm	Attributes	Applicable major release
Name: SgNBCommon_spareAlarmSgNBCommon6 (13011) Type: equipmentAlarm Package: femto.SgNBCommon_ spareAlarmSgNBCommon6 Raised on class: femto.SgNBCommon	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm 6		

Table 28-505 SS7LinkSet_congestionTowardsRemoteMTP3

Alarm	Attributes	Applicable major release
Name: SS7LinkSet_congestionTowardsRemoteMTP3 (6214) Type: qualityOfServiceAlarm Package: femto.SS7LinkSet_ congestionTowardsRemoteMTP3 Raised on class: femto.SS7LinkSet	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: congestion	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Congestion at the MTP3 layer towards the peer node, as the traffic on the signalling link is beyond the capacity.		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-506 SS7LinkSet_remoteMTP3Unreachable

Alarm	Attributes	Applicable major release
Name: SS7LinkSet_remoteMTP3Unreachable (6215) Type: communicationsAlarm Package: femto.SS7LinkSet_ remoteMTP3Unreachable Raised on class: femto.SS7LinkSet	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The peer node is unreachable as no MTP3 link is available in service on this interface.		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-507 SS7Link_mtp3LinkDown

Alarm	Attributes	Applicable major release
Name: SS7Link_mtp3LinkDown (6216) Type: communicationsAlarm Package: femto.SS7Link_mtp3LinkDown Raised on class: femto.SS7Link	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: MTP3 Link is down		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-508 SS7Link_mtp3LinkRemotelyBlocked

Alarm	Attributes	Applicable major release
Name: SS7Link_mtp3LinkRemotelyBlocked (6217) Type: communicationsAlarm Package: femto.SS7Link_mtp3LinkRemotelyBlocked Raised on class: femto.SS7Link	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteNodeTransmissionError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The peer node has blocked the traffic on this MTP3 link		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-509 SS7Link_qsaalLinkCongested

Alarm	Attributes	Applicable major release
Name: SS7Link_qsaalLinkCongested (6218) Type: qualityOfServiceAlarm Package: femto.SS7Link_qsaalLinkCongested Raised on class: femto.SS7Link	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: congestion	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The traffic on the SSCF-NNI link has exceeded the congestion threshold		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-510 SS7Stack_sS7StackFailure

Alarm	Attributes	Applicable major release
Name: SS7Stack_sS7StackFailure (6219) Type: processingErrorAlarm Package: femto.SS7Stack_sS7StackFailure Raised on class: femto.SS7Stack	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: SS7 Stack bringup failure or the SP hosting the SS7 Stack Instance is down in distributed mode		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-511 SS7Stack_trilliumBuffersBelowThreshold

Alarm	Attributes	Applicable major release
Name: SS7Stack_trilliumBuffersBelowThreshold (6220) Type: processingErrorAlarm Package: femto.SS7Stack_ trilliumBuffersBelowThreshold Raised on class: femto.SS7Stack	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Available Trillium Buffers are below threshold		
Remedial action: N/A this alarm will not be raised in this release.		

Table 28-512 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 28-513 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 28-514 SubscriberTraceConfig_subscriberTraceRecordingSessionFailure

Alarm	Attributes	Applicable major release
Name: SubscriberTraceConfig_ subscriberTraceRecordingSessionFailure (6242) Type: processingErrorAlarm Package: femto.SubscriberTraceConfig_ subscriberTraceRecordingSessionFailure Raised on class: femto.SubscriberTraceConfiguration	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Failure to start a trace recording session due to any problem		
Remedial action: Configure the IMSI attribute of class SubscriberTrace and perform the call trace recording session.Verify the call of the IMSI to be traced.The alarms gets cleared manually from SAM once the call is traced by the clear alarm. SUBSCRIBERTRACECONFIG_SUBSCRIBERTRACERECORDINGSESSIONFAILURECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-515 SubscriberTraceConfig_subscriberTraceUploadFailure

Alarm	Attributes	Applicable major release
Name: SubscriberTraceConfig_ subscriberTraceUploadFailure (6243) Type: communicationsAlarm Package: femto.SubscriberTraceConfig_ subscriberTraceUploadFailure Raised on class: femto.SubscriberTraceConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: responseTimeExcessive	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: Failure to transferring Call Trace files even after retries		

Table 28-515 SubscriberTraceConfig_subscriberTraceUploadFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Configure the IMSIattribute of the class SubscriberTrace and perform the call trace recording session.Verify the call of the IMSI to be traced.Verify the subscriber record files that are uploaded to the SFTP server defined by the attributes sftpServer and rootDirectoryof a class SubscriberTraceConfig.		

Table 28-516 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 28-517 SwitchBlade_unsupportedRtm

Alarm	Attributes	Applicable major release
Name: SwitchBlade_unsupportedRtm (8501) Type: equipmentAlarm Package: femto.SwitchBlade_unsupportedRtm Raised on class: femto.SwitchBlade	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitTypeMismatch	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when an unsupported RTM is used		
Remedial action: Check RTM type used		

Table 28-518 SwitchBlade_unsupportedSwitchBladeCombination

Alarm	Attributes	Applicable major release
Name: SwitchBlade_ unsupportedSwitchBladeCombination (8502) Type: equipmentAlarm Package: femto.SwitchBlade_ unsupportedSwitchBladeCombination Raised on class: femto.SwitchBlade	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableUnitTypeMismatch	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when two incompatible switch blades are used. Note: This may happen as part of upgrade process, which is acceptable.		
Remedial action: Check switchblades used		

Table 28-519 SwitchPort_interfaceFailure

Alarm	Attributes	Applicable major release
Name: SwitchPort_interfaceFailure (8503) Type: equipmentAlarm Package: femto.SwitchPort_interfaceFailure Raised on class: femto.SwitchPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when a EthernetIntf interface failure occurs.		
Remedial action: Check the connectivity to the Ethernet port. The alarm gets cleared once the connectivity is restored.		

Table 28-520 TOD_externalClockReferenceFailure

Alarm	Attributes	Applicable major release
Name: TOD_externalClockReferenceFailure (6244) Type: communicationsAlarm Package: femto.TOD_externalClockReferenceFailure Raised on class: femto.TOD	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: timingProblem	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when an external SNTP server is configured but it is out of service. The system time is in free-running mode using the local oscillator and the operator needs to take care that the ToD value for the Femto Cluster is using the right value.		
Remedial action: Check the status of the external SNTP server		

Table 28-521 TOD_sntpServerDownNode1

Alarm	Attributes	Applicable major release
Name: TOD_sntpServerDownNode1 (6245) Type: processingErrorAlarm Package: femto.TOD_sntpServerDownNode1 Raised on class: femto.TOD	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the ToD server within SCGW Node1 is out of service.		
Remedial action: Enter the command ps -ef | grep ntpd to verify whether the SNTP service is running on the Gateway server.		

Table 28-522 TOD_sntpServerDownNode2

Alarm	Attributes	Applicable major release
Name: TOD_sntpServerDownNode2 (6246) Type: processingErrorAlarm Package: femto.TOD_sntpServerDownNode2 Raised on class: femto.TOD	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: outOfService	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when the ToD server within SCGW Node2 is out of service.		
Remedial action: Enter the command ps -ef | grep ntpd to verify whether the SNTP service is running on the Gateway server.		

Table 28-523 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 28-524 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 28-525 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		

Table 28-525 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 28-526 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 28-527 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 28-528 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 28-529 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 28-530 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		

Table 28-530 UplinkDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 28-531 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 28-532 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 28-533 VirtualMachineDiskPartition_vMachineDiskPartitionNearingCapacity

Alarm	Attributes	Applicable major release
Name: VirtualMachineDiskPartition_ vMachineDiskPartitionNearingCapacity (12407) Type: equipmentAlarm Package: femto.VirtualMachineDiskPartition_ vMachineDiskPartitionNearingCapacity Raised on class: femto.VirtualMachineDiskPartition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the disk partition usage has exceeded seventy percent of available capacity. The alarm is automatically cleared whenever disk partition usage is reduced below thirty percent of available capacity.		
Remedial action: Check or correct the disk usage in the identified partition.		

Table 28-534 VirtualMachineDisk_vDiskUsageNearingCapacity

Alarm	Attributes	Applicable major release
Name: VirtualMachineDisk_ vDiskUsageNearingCapacity (12408) Type: equipmentAlarm Package: femto.VirtualMachineDisk_ vDiskUsageNearingCapacity Raised on class: femto.VirtualMachineDisk	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is raised whenever the disk usage has exceeded seventy percent of available capacity. The alarm is automatically cleared whenever disk usage is reduced below thirty percent of available capacity.		
Remedial action: Cleanup unnecessary backups,files to bring down disk usage		

Table 28-535 VirtualMachineInterface_vLANInterfaceDown

Alarm	Attributes	Applicable major release
Name: VirtualMachineInterface_vLANInterfaceDown (12409) Type: communicationsAlarm Package: femto.VirtualMachineInterface_ vLANInterfaceDown Raised on class: femto.VirtualMachineInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault indicates that VLAN is not reachable and it is not active.		
Remedial action: Ensure that the VLAN is properly configured on all the next hops, switches and routers.The fault is automatically cleared by the alarmVIRTUALMACHINEINTERFACE_VLANINTERFACEDOWNCLEARANCE.If alarm persists, contact Nokia customer support.		

Table 28-536 VirtualMachineNextHopHB_fgwActiveSRLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualMachineNextHopHB_ fgwActiveSRLinkDown (12411) Type: communicationsAlarm Package: femto.VirtualMachineNextHopHB_ fgwActiveSRLinkDown Raised on class: femto.VirtualMachineNextHopHB	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that SCGW Active node cannot reach one of the SRs connected to it. This alarm shall be raised for each SR failure		
Remedial action: Check the connection between the gateway and the service router for the active SR linkIf the problem persists, contact Nokia customer support.		

Table 28-537 VirtualMachineNextHopHB_fgwStandbySRLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualMachineNextHopHB_ fgwStandbySRLinkDown (12412) Type: communicationsAlarm Package: femto.VirtualMachineNextHopHB_ fgwStandbySRLinkDown Raised on class: femto.VirtualMachineNextHopHB	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This alarm is reported to indicate that SCGW Standby node cannot reach one of the SRs connected to it. This alarm shall be raised for each SR failure		
Remedial action: Check the connection between the gateway and the service router for the standby SR Link. If the problem persists, contact Nokia customer support.		

Table 28-538 VirtualMachineNIC_vNetworkInterfaceFailure

Alarm	Attributes	Applicable major release
Name: VirtualMachineNIC_vNetworkInterfaceFailure (12410) Type: equipmentAlarm Package: femto.VirtualMachineNIC_ vNetworkInterfaceFailure Raised on class: femto.VirtualMachineNIC	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: This fault is generated when a virtual Network interface failure occurs for vFGW.		
Remedial action: Identify the root cause of network port failure.This fault is cleared automatically by the clear alarmVIRTUALMACHINENIC_VNETWORKINTERFACEFAILURECLEARANCE.If the problem persists, contact Nokia customer support.		

Table 28-539 VirtualMachineServer_spareAlarmVirtualMachineServer1

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer1 (12413) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer1 Raised on class: femto.VirtualMachineServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 1		
Remedial action: Spare Alarm 1		

Table 28-540 VirtualMachineServer_spareAlarmVirtualMachineServer2

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer2 (12414) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer2 Raised on class: femto.VirtualMachineServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 2		
Remedial action: Spare Alarm 2		

Table 28-541 VirtualMachineServer_spareAlarmVirtualMachineServer3

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer3 (12415) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer3 Raised on class: femto.VirtualMachineServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 3		
Remedial action: Spare Alarm 3		

Table 28-542 VirtualMachineServer_spareAlarmVirtualMachineServer4

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer4 (12416) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer4 Raised on class: femto.VirtualMachineServer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 4		
Remedial action: Spare Alarm 4		

Table 28-543 VirtualMachineServer_spareAlarmVirtualMachineServer5

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer5 (12417) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer5 Raised on class: femto.VirtualMachineServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC17.2 • SC19.1 • SC20.1
Description: Spare Alarm 5		
Remedial action: Spare Alarm 5		

Table 28-544 VirtualMachineServer_spareAlarmVirtualMachineServer6

Alarm	Attributes	Applicable major release
Name: VirtualMachineServer_ spareAlarmVirtualMachineServer6 (12972) Type: equipmentAlarm Package: femto.VirtualMachineServer_ spareAlarmVirtualMachineServer6 Raised on class: femto.VirtualMachineServer	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • SC19.1 • SC20.1
Description: Spare Alarm 6		
Remedial action: Spare Alarm 6		

Table 28-545 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • SC17.2 • SC19.1 • SC20.1 • 4.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

29 9xxx eNodeB

29.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 29-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 29-2 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 29-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 29-4 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 29-5 BackupRestoreApplicationLockNotObtained

Alarm	Attributes	Applicable major release
Name: BackupRestoreApplicationLockNotObtained (1962) Type: integrityViolation Package: lte. BackupRestoreApplicationLockNotObtained Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnableToAcquireLock	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the Backup/Restore Application is unable to acquire lock. Retry the Backup/Restore Operation once the lock is released by the other application.		

Table 29-5 BackupRestoreApplicationLockNotObtained (continued)

Alarm	Attributes	Applicable major release
Remedial action: Retry the Backup/Restore Operation once the lock is released by the other application.		

Table 29-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 29-7 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 29-8 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 29-9 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 29-10 BscAccessAdminDown

Alarm	Attributes	Applicable major release
Name: BscAccessAdminDown (4629) Type: equipmentAlarm Package: lte.BscAccessAdminDown Raised on class: lte.BscAccess	Severity: warning Specific problem: BSC Access LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a BSC Access Administrative State is down.		
Raising condition: (('administrativeState' NOT EQUAL 'Unlocked'))		
Clearing condition: (('administrativeState' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-11 BsCommunicationStateOffline

Alarm	Attributes	Applicable major release
Name: BsCommunicationStateOffline (1264) Type: communicationsAlarm Package: lte.BsCommunicationStateOffline Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bsCommunicationOffline	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the BS Communication State goes 'offline'. While BS communication state is 'offline' none of the SNMP properties can be set.		
Raising condition: (('bsCommunicationState' NOT EQUAL 'omcManaged'))		
Clearing condition: (('bsCommunicationState' EQUAL 'omcManaged'))		
Remedial action: Will come back online when the NEM session is closed.		

Table 29-12 CallTraceAlreadyActive

Alarm	Attributes	Applicable major release
Name: CallTraceAlreadyActive (1279) Type: callTraceSessionAlarm Package: lte.CallTraceAlreadyActive Raised on class: lte.CTg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: callTraceManuallyActivated	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a Call Trace Session is already active when the scheduled task starts. The scheduled task will not deactivate it. The Call Trace Session must be manually deactivated. The alarm is cleared when the Call Trace session is deactivated successfully.		
Remedial action: The existing Call Trace Session must be manually deactivated. The alarm is cleared when the Call Trace session is deactivated successfully.		

Table 29-13 CallTraceScheduledTaskExecutionError

Alarm	Attributes	Applicable major release
Name: CallTraceScheduledTaskExecutionError (1280) Type: callTraceSessionAlarm Package: lte.CallTraceScheduledTaskExecutionError Raised on class: lte.CTg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: callTraceConfigurationError Applicable probable causes: • callTraceConfigurationError • eventBasedTraceEnabled • debugTraceActive	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the execution of a Call Trace scheduled task has a failure activating or deactivating this Call Trace session.		
Remedial action: Check the call trace session.		

Table 29-14 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 29-15 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		

Table 29-15 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 29-16 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 29-17 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 29-18 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 29-19 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 29-20 CTAuxMisalignementWhileEnbAutoAllocationDisabled

Alarm	Attributes	Applicable major release
Name: CTAuxMisalignementWhileEnbAutoAllocationDisabled (5423) Type: communicationsAlarm Package: lte.CTAuxMisalignementWhileEnbAutoAllocationDisabled Raised on class: lte.CallTraceSessionManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: eNBsAuxIPMisalignment	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-20 CTAuxMisalignementWhileEnbAutoAllocationDisabled (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised if automatic AUX allocation is disabled and if there is a discrepancy between the eNB configurations and the AUX assigned to the eNB in SAM. If the automatic AUX allocation is enabled, SAM will automatically set the eNB IP addresses linked to the trace management on the assigned AUX in SAM.		
Remedial action: Manually launch the allocation of the eNBs to the active CT AUX server.		

Table 29-21 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 29-22 ENBEquipmentAdminDown

Alarm	Attributes	Applicable major release
Name: ENBEquipmentAdminDown (1359) Type: equipmentAlarm Package: lte.ENBEquipmentAdminDown Raised on class: lte.ENBEquipment	Severity: warning Specific problem: ENBEquipment LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an ENB Equipment Administrative State is down.		
Raising condition: (('administrativeState' NOT EQUAL 'Unlocked'))		
Clearing condition: (('administrativeState' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-23 ENBEquipmentDegraded

Alarm	Attributes	Applicable major release
Name: ENBEquipmentDegraded (9557) Type: equipmentAlarm Package: lte.ENBEquipmentDegraded Raised on class: lte.ENBEquipment	Severity: major Specific problem: ENBEquipment DEGRADED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an ENB Equipment is not fully available.		
Raising condition: ('availabilityStatus'anyBit'Degraded')		
Clearing condition: NOT (('availabilityStatus'anyBit'Degraded'))		
Remedial action: The Equipment is not fully available. AvailabilityStatus value and Additional attributes may indicate the nature and cause of the issue.		

Table 29-24 ENBEquipmentDown

Alarm	Attributes	Applicable major release
Name: ENBEquipmentDown (1360) Type: equipmentAlarm Package: lte.ENBEquipmentDown Raised on class: lte.ENBEquipment	Severity: critical Specific problem: ENBEquipment DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an ENB Equipment is operationally down.		
Raising condition: (('operationalState' NOT EQUAL 'Enabled') AND ('administrativeState' EQUAL 'Unlocked') AND (('availabilityStatus'anyBit'Failed') OR ('availabilityStatus'anyBit'Dependency')))		
Clearing condition: ((('administrativeState' EQUAL 'Locked') OR ('operationalState' EQUAL 'Enabled') OR NOT ((('availabilityStatus'anyBit'Failed') OR ('availabilityStatus'anyBit'Dependency'))))		
Remedial action: The Equipment is inoperable. Additional attributes may indicate the nature and cause of the issue.		

Table 29-25 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		

Table 29-25 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 29-26 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 29-27 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 29-28 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 29-29 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 29-30 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 29-31 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 29-32 FRUAdminDown

Alarm	Attributes	Applicable major release
Name: FRUAdminDown (2919) Type: equipmentAlarm Package: lte.FRUAdminDown Raised on class: lte.FRU	Severity: warning Specific problem: FRU LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an ENB FRU Administrative State is down		
Raising condition: (('Administrative State' NOT EQUAL 'Unlocked'))		
Clearing condition: (('Administrative State' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-33 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 29-33 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 29-34 IK4001001

Alarm	Attributes	Applicable major release
Name: IK4001001 (2122) Type: equipmentAlarm Package: lte.IK4001001 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to read the TMA manufacturer data record.		
Remedial action: Check the TMA or the AISG communication bus		

Table 29-35 IK4001002

Alarm	Attributes	Applicable major release
Name: IK4001002 (2123) Type: equipmentAlarm Package: lte.IK4001002 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-36 IK4001003

Alarm	Attributes	Applicable major release
Name: IK4001003 (2124) Type: equipmentAlarm Package: lte.IK4001003 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-37 IK4001004

Alarm	Attributes	Applicable major release
Name: IK4001004 (2125) Type: equipmentAlarm Package: lte.IK4001004 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-38 IK4001005

Alarm	Attributes	Applicable major release
Name: IK4001005 (2126) Type: equipmentAlarm Package: lte.IK4001005 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-39 IK4001006

Alarm	Attributes	Applicable major release
Name: IK4001006 (2127) Type: equipmentAlarm Package: lte.IK4001006 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-40 IK4001007

Alarm	Attributes	Applicable major release
Name: IK4001007 (2128) Type: equipmentAlarm Package: lte.IK4001007 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALARM MINOR SUB6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-40 IK4001007 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a minor TMA subunit fault which reduces gain performance but maintains its function.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-41 IK4001008

Alarm	Attributes	Applicable major release
Name: IK4001008 (2129) Type: equipmentAlarm Package: lte.IK4001008 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-42 IK4001009

Alarm	Attributes	Applicable major release
Name: IK4001009 (2130) Type: equipmentAlarm Package: lte.IK4001009 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-43 IK4001010

Alarm	Attributes	Applicable major release
Name: IK4001010 (2131) Type: equipmentAlarm Package: lte.IK4001010 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-44 IK4001011

Alarm	Attributes	Applicable major release
Name: IK4001011 (2132) Type: equipmentAlarm Package: lte.IK4001011 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-45 IK4001012

Alarm	Attributes	Applicable major release
Name: IK4001012 (2133) Type: equipmentAlarm Package: lte.IK4001012 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-46 IK4001013

Alarm	Attributes	Applicable major release
Name: IK4001013 (2134) Type: equipmentAlarm Package: lte.IK4001013 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA ALARM MAJOR SUB6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-47 IK4001014

Alarm	Attributes	Applicable major release
Name: IK4001014 (2135) Type: equipmentAlarm Package: lte.IK4001014 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA ALD UNIT SUPPORT WRONG AISG VERSION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-47 IK4001014 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the ALD unit does not support AISG version 2.0.		
Remedial action: Upgrade the TMA software or replace it with an AISG v2.0 unit.		

Table 29-48 IK4001015

Alarm	Attributes	Applicable major release
Name: IK4001015 (2136) Type: equipmentAlarm Package: lte.IK4001015 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA LOSS OF COMM Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L
Description: This alarm indicates the RFM that acts as an AISG Controller has lost communication to the TMA unit.		
Remedial action: Reset the ASIG-host RFM, inspect and repair the AISG bus, or replace the TMA.		

Table 29-49 IK4001017

Alarm	Attributes	Applicable major release
Name: IK4001017 (2960) Type: equipmentAlarm Package: lte.IK4001017 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-50 IK4001018

Alarm	Attributes	Applicable major release
Name: IK4001018 (2961) Type: equipmentAlarm Package: lte.IK4001018 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-51 IK4001019

Alarm	Attributes	Applicable major release
Name: IK4001019 (2962) Type: equipmentAlarm Package: lte.IK4001019 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-52 IK4001020

Alarm	Attributes	Applicable major release
Name: IK4001020 (2963) Type: equipmentAlarm Package: lte.IK4001020 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-53 IK4001021

Alarm	Attributes	Applicable major release
Name: IK4001021 (2964) Type: equipmentAlarm Package: lte.IK4001021 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA HW FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a general TMA HW failure.		
Remedial action: Replace the TMA.		

Table 29-54 IK4001022

Alarm	Attributes	Applicable major release
Name: IK4001022 (2965) Type: equipmentAlarm Package: lte.IK4001022 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA BYPASS MODE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that TMA is in bypass mode and is not providing RF gain.		

Table 29-54 IK4001022 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If TMA fault is present then replace TMA, otherwise set TMA to Bypass Off (when supported).		

Table 29-55 IK4001030

Alarm	Attributes	Applicable major release
Name: IK4001030 (3749) Type: equipmentAlarm Package: lte.IK4001030 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the unit is automatically reset to attempt to clear the fault. If the problem persists then replace the failed TMA.		
Remedial action: The unit is automatically reset to attempt to clear the fault. If the problem persists then replace the failed TMA.		

Table 29-56 IK4001031

Alarm	Attributes	Applicable major release
Name: IK4001031 (5192) Type: equipmentAlarm Package: lte.IK4001031 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a failure of the TMA has been detected that cannot described by any specific alarm.		
Remedial action: If the failure affects the RF portion of the TMA then the receive RF gain on the path(s) served by the TMA is reduced. If the failure affects only the AISG terminal function of the TMA then RF gain should still be active.		

Table 29-57 IK4001032

Alarm	Attributes	Applicable major release
Name: IK4001032 (8504) Type: equipmentAlarm Package: lte.IK4001032 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-58 IK4001033

Alarm	Attributes	Applicable major release
Name: IK4001033 (8505) Type: equipmentAlarm Package: lte.IK4001033 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-59 IK4001034

Alarm	Attributes	Applicable major release
Name: IK4001034 (8506) Type: equipmentAlarm Package: lte.IK4001034 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-60 IK4001035

Alarm	Attributes	Applicable major release
Name: IK4001035 (8507) Type: equipmentAlarm Package: lte.IK4001035 Raised on classes: • lte.RetAldEntry • lte.BBCardSpecifics • lte.ENBEquipment • lte.TmaAldEntry • lte.Rae	Severity: major Specific problem: LOSS OF COMM Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The communication to the reporting hardware module has been lost.		
Remedial action: Reset the alarmed module; if unsuccessful, reset the eNodeB. If communication cannot be restored, replace the faulty hardware module.		

Table 29-61 IK4001036

Alarm	Attributes	Applicable major release
Name: IK4001036 (8508) Type: equipmentAlarm Package: lte.IK4001036 Raised on classes: • lte.RFM • lte.ENBShelfSpecifics • lte.RFME • lte.RetAldEntry • lte.MODULE • lte.ENBEquipment • lte.AMR • lte.TmaAldEntry	Severity: minor Specific problem: UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to read the manufacturer data record.		
Remedial action: Reset or replace the concerned hardware if possible, or call the next level of support		

Table 29-62 IK4001037

Alarm	Attributes	Applicable major release
Name: IK4001037 (8509) Type: equipmentAlarm Package: lte.IK4001037 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: major Specific problem: HW FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a general HW failure.		
Remedial action: Replace the unit.		

Table 29-63 IK4001038

Alarm	Attributes	Applicable major release
Name: IK4001038 (8510) Type: equipmentAlarm Package: lte.IK4001038 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		

Table 29-63 IK4001038 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-64 IK4001039

Alarm	Attributes	Applicable major release
Name: IK4001039 (8511) Type: equipmentAlarm Package: lte.IK4001039 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-65 IK4001040

Alarm	Attributes	Applicable major release
Name: IK4001040 (8512) Type: equipmentAlarm Package: lte.IK4001040 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-66 IK4001041

Alarm	Attributes	Applicable major release
Name: IK4001041 (8513) Type: equipmentAlarm Package: lte.IK4001041 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-67 IK4001042

Alarm	Attributes	Applicable major release
Name: IK4001042 (8514) Type: equipmentAlarm Package: lte.IK4001042 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-68 IK4001043

Alarm	Attributes	Applicable major release
Name: IK4001043 (8515) Type: equipmentAlarm Package: lte.IK4001043 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA IN_BYPASS SUB6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a major TMA subunit fault which prevents its function. More details are in additional info.		
Remedial action: Reset the TMA, if problem persists then replace the TMA.		

Table 29-69 IK4001044

Alarm	Attributes	Applicable major release
Name: IK4001044 (10041) Type: equipmentAlarm Package: lte.IK4001044 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TMA EVENT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		
Remedial action: No action is required.		

Table 29-70 IK4001045

Alarm	Attributes	Applicable major release
Name: IK4001045 (10042) Type: equipmentAlarm Package: lte.IK4001045 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TMA EVENT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified TMA fault detected		

Table 29-70 IK4001045 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-71 IK4002001

Alarm	Attributes	Applicable major release
Name: IK4002001 (2137) Type: equipmentAlarm Package: lte.IK4002001 Raised on class: lte.AMR	Severity: minor Specific problem: AMR INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to initialize the RF cabinet alarm module.		
Remedial action: Check the cabling between TRDU and AMR. If the alarm persists, reset one or more of the TRDUs, or replace the AMR.		

Table 29-72 IK4002002

Alarm	Attributes	Applicable major release
Name: IK4002002 (2138) Type: equipmentAlarm Package: lte.IK4002002 Raised on class: lte.AMR	Severity: minor Specific problem: AMR COMM FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the loss of communication with RF cabinet Alarm Module.		
Remedial action: Check the cabling between TRDU and AMR. If the alarm persists, reset one or more of the TRDUs, or replace the AMR.		

Table 29-73 IK4002003

Alarm	Attributes	Applicable major release
Name: IK4002003 (2139) Type: equipmentAlarm Package: lte.IK4002003 Raised on class: lte.AMR	Severity: warning Specific problem: AMR UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to read the RF cabinet alarm module manufacturer data.		
Remedial action: Check the cabling between TRDU and AMR. If the alarm persists, reset one or more of the TRDUs, or replace the AMR.		

Table 29-74 IK4002004

Alarm	Attributes	Applicable major release
Name: IK4002004 (2140) Type: equipmentAlarm Package: lte.IK4002004 Raised on class: lte.AMR	Severity: major Specific problem: AMR FAN ALARM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet fan is out of service.		
Remedial action: Replace the fan of the RF cabinet.		

Table 29-75 IK4002005

Alarm	Attributes	Applicable major release
Name: IK4002005 (2141) Type: environmentalAlarm Package: lte.IK4002005 Raised on class: lte.AMR	Severity: minor Specific problem: AMR DOOR ALARM Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet door is open.		
Remedial action: Close the cabinet door.		

Table 29-76 IK4002006

Alarm	Attributes	Applicable major release
Name: IK4002006 (2142) Type: environmentalAlarm Package: lte.IK4002006 Raised on class: lte.AMR	Severity: major Specific problem: AMR OVER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet temperature is above the safe operating temperature.		
Remedial action: Check the cabinet for proper functioning fans and clean air filters. Check if the ambient temperature is within the recommended operating range.		

Table 29-77 IK4002007

Alarm	Attributes	Applicable major release
Name: IK4002007 (2143) Type: equipmentAlarm Package: lte.IK4002007 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAF Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L

Table 29-77 IK4002007 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RF cabinet filter airflow is reduced.		
Remedial action: Replace the fresh air filter.		

Table 29-78 IK4002016

Alarm	Attributes	Applicable major release
Name: IK4002016 (2966) Type: equipmentAlarm Package: lte.IK4002016 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-79 IK4002017

Alarm	Attributes	Applicable major release
Name: IK4002017 (2967) Type: equipmentAlarm Package: lte.IK4002017 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-80 IK4002018

Alarm	Attributes	Applicable major release
Name: IK4002018 (2968) Type: equipmentAlarm Package: lte.IK4002018 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-81 IK4002019

Alarm	Attributes	Applicable major release
Name: IK4002019 (2969) Type: equipmentAlarm Package: lte.IK4002019 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-82 IK4002020

Alarm	Attributes	Applicable major release
Name: IK4002020 (2970) Type: equipmentAlarm Package: lte.IK4002020 Raised on class: lte.AMR	Severity: minor Specific problem: AMR FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-83 IK4002021

Alarm	Attributes	Applicable major release
Name: IK4002021 (8516) Type: equipmentAlarm Package: lte.IK4002021 Raised on class: lte.AMR	Severity: major Specific problem: AMR FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-84 IK4002022

Alarm	Attributes	Applicable major release
Name: IK4002022 (8517) Type: equipmentAlarm Package: lte.IK4002022 Raised on class: lte.AMR	Severity: major Specific problem: AMR FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-84 IK4002022 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. An unspecified AMR fault has been detected.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-85 IK4002023

Alarm	Attributes	Applicable major release
Name: IK4002023 (10043) Type: equipmentAlarm Package: lte.IK4002023 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR event has been detected.		
Remedial action: No action is required.		

Table 29-86 IK4002024

Alarm	Attributes	Applicable major release
Name: IK4002024 (10044) Type: equipmentAlarm Package: lte.IK4002024 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR event has been detected.		
Remedial action: No action is required.		

Table 29-87 IK4002025

Alarm	Attributes	Applicable major release
Name: IK4002025 (10045) Type: equipmentAlarm Package: lte.IK4002025 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. An unspecified AMR event has been detected.		
Remedial action: No action is required.		

Table 29-88 IK4003003

Alarm	Attributes	Applicable major release
Name: IK4003003 (2152) Type: equipmentAlarm Package: lte.IK4003003 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the BB initialization failure.		
Remedial action: Reset BB. Use the reset command on the SAM, or reset using the remote connection to NEM. If the alarm persists, replace BB.		

Table 29-89 IK4003006

Alarm	Attributes	Applicable major release
Name: IK4003006 (5196) Type: equipmentAlarm Package: lte.IK4003006 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a failure of the modem (baseband unit) has been detected that cannot described by any specific alarm.		
Remedial action: The unit is automatically reset to attempt to clear the fault. If the problem persists then replace the failed modem.		

Table 29-90 IK4003008

Alarm	Attributes	Applicable major release
Name: IK4003008 (2153) Type: communicationsAlarm Package: lte.IK4003008 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB LOSS OF COMM Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L
Description: This alarm indicates the loss of layer 3 communication to the modem.		
Remedial action: If the alarm persists for more than 15 minutes, then perform the following tasks sequentially until the alarm clears. Please allow 10 minutes for the alarm to clear after each task. \n\n1. Check the state of the CEM. If "Initializing" is indicated then another 10 minutes should be allowed to pass before resetting the BB. \n2. Reset the BB via NEM. \n3. Check if BB is present in the cabinet, remove and reinsert BB. \n4. Replace BB. \n5. Check the back panel and replace CB. \n6. Call next level of support.		

Table 29-91 IK4003042

Alarm	Attributes	Applicable major release
Name: IK4003042 (2154) Type: equipmentAlarm Package: lte.IK4003042 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB FAULT BIST FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Built In Self Test failure.		
Remedial action: Reset BB, replace if problem persist		

Table 29-92 IK4003043

Alarm	Attributes	Applicable major release
Name: IK4003043 (2155) Type: processingErrorAlarm Package: lte.IK4003043 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software download failure.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-93 IK4003044

Alarm	Attributes	Applicable major release
Name: IK4003044 (2156) Type: equipmentAlarm Package: lte.IK4003044 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB OVER TEMP MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the modem temperature is rising to the shutdown limit.		
Remedial action: Check for proper fan operation and that the fan type is compatible with the BB type, check that DBU inlet temperature is within operating range.		

Table 29-94 IK4003045

Alarm	Attributes	Applicable major release
Name: IK4003045 (2157) Type: equipmentAlarm Package: lte.IK4003045 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB OVER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the modem temperature is above operating range.		

Table 29-94 IK4003045 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check for proper fan operation and that the fan type is compatible with the BB type, check that DBU inlet temperature is within operating range.		

Table 29-95 IK4003046

Alarm	Attributes	Applicable major release
Name: IK4003046 (2158) Type: processingErrorAlarm Package: lte.IK4003046 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB SOFTWARE FAIL Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a general platform software failure.		
Remedial action: Reset the BB.		

Table 29-96 IK4003048

Alarm	Attributes	Applicable major release
Name: IK4003048 (2160) Type: equipmentAlarm Package: lte.IK4003048 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB L1 HARDWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware failure.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-97 IK4003050

Alarm	Attributes	Applicable major release
Name: IK4003050 (2162) Type: processingErrorAlarm Package: lte.IK4003050 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 1 software warning.		
Remedial action: Reset the BB in low traffic hours.		

Table 29-98 IK4003051

Alarm	Attributes	Applicable major release
Name: IK4003051 (2163) Type: processingErrorAlarm Package: lte.IK4003051 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L2 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 2 software warning.		
Remedial action: Reset the BB in low traffic hours.		

Table 29-99 IK4003052

Alarm	Attributes	Applicable major release
Name: IK4003052 (2164) Type: equipmentAlarm Package: lte.IK4003052 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB L2 HARDWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a Layer 2 hardware failure.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-100 IK4003053

Alarm	Attributes	Applicable major release
Name: IK4003053 (2165) Type: communicationsAlarm Package: lte.IK4003053 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB LOSS OF HS DATA LINK ALL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of high-speed data links to all BBs.		
Remedial action: Reset the BB and/or eNodeB, if problem persists then replace the BB or CB.		

Table 29-101 IK4003054

Alarm	Attributes	Applicable major release
Name: IK4003054 (2166) Type: equipmentAlarm Package: lte.IK4003054 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB LED FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to control face-plate LEDs.		
Remedial action: Reset the BB in low traffic hours.		

Table 29-102 IK4003055

Alarm	Attributes	Applicable major release
Name: IK4003055 (2167) Type: equipmentAlarm Package: lte.IK4003055 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB NON CPU POWER FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a BB power failure to the peripheral devices except the Ethernet switch and the P4080.		
Remedial action: Replace the BB.		

Table 29-103 IK4003056

Alarm	Attributes	Applicable major release
Name: IK4003056 (2168) Type: equipmentAlarm Package: lte.IK4003056 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB HS DATA LINK SYNC FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to synchronize SFN to modem.		
Remedial action: Reset the BB.		

Table 29-104 IK4003057

Alarm	Attributes	Applicable major release
Name: IK4003057 (2169) Type: processingErrorAlarm Package: lte.IK4003057 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		
Remedial action: Reset the BB.		

Table 29-105 IK4003058

Alarm	Attributes	Applicable major release
Name: IK4003058 (2170) Type: processingErrorAlarm Package: lte.IK4003058 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		

Table 29-105 IK4003058 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the BB.		

Table 29-106 IK4003059

Alarm	Attributes	Applicable major release
Name: IK4003059 (2171) Type: processingErrorAlarm Package: lte.IK4003059 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		
Remedial action: Reset the BB.		

Table 29-107 IK4003060

Alarm	Attributes	Applicable major release
Name: IK4003060 (2172) Type: processingErrorAlarm Package: lte.IK4003060 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		
Remedial action: Reset the BB.		

Table 29-108 IK4003061

Alarm	Attributes	Applicable major release
Name: IK4003061 (2173) Type: processingErrorAlarm Package: lte.IK4003061 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		
Remedial action: Reset the BB.		

Table 29-109 IK4003062

Alarm	Attributes	Applicable major release
Name: IK4003062 (2174) Type: processingErrorAlarm Package: lte.IK4003062 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the BB.		
Remedial action: Reset the BB.		

Table 29-110 IK4003063

Alarm	Attributes	Applicable major release
Name: IK4003063 (2175) Type: equipmentAlarm Package: lte.IK4003063 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 HARDWARE FAIL SLICE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a hardware failure on the BB.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-111 IK4003064

Alarm	Attributes	Applicable major release
Name: IK4003064 (2176) Type: equipmentAlarm Package: lte.IK4003064 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 HARDWARE FAIL SLICE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a hardware failure on the BB.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-112 IK4003065

Alarm	Attributes	Applicable major release
Name: IK4003065 (2177) Type: equipmentAlarm Package: lte.IK4003065 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 HARDWARE FAIL SLICE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a hardware failure on the BB.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-113 IK4003066

Alarm	Attributes	Applicable major release
Name: IK4003066 (2178) Type: processingErrorAlarm Package: lte.IK4003066 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-114 IK4003067

Alarm	Attributes	Applicable major release
Name: IK4003067 (2179) Type: processingErrorAlarm Package: lte.IK4003067 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-115 IK4003068

Alarm	Attributes	Applicable major release
Name: IK4003068 (2180) Type: processingErrorAlarm Package: lte.IK4003068 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-116 IK4003069

Alarm	Attributes	Applicable major release
Name: IK4003069 (2181) Type: processingErrorAlarm Package: lte.IK4003069 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L2 SOFTWARE WARNING SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-116 IK4003069 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-117 IK4003070

Alarm	Attributes	Applicable major release
Name: IK4003070 (2182) Type: processingErrorAlarm Package: lte.IK4003070 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L2 SOFTWARE WARNING SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-118 IK4003071

Alarm	Attributes	Applicable major release
Name: IK4003071 (2183) Type: processingErrorAlarm Package: lte.IK4003071 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L2 SOFTWARE WARNING SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		
Remedial action: Reset BB in low traffic hours.		

Table 29-119 IK4003075

Alarm	Attributes	Applicable major release
Name: IK4003075 (2974) Type: equipmentAlarm Package: lte.IK4003075 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-120 IK4003076

Alarm	Attributes	Applicable major release
Name: IK4003076 (2975) Type: equipmentAlarm Package: lte.IK4003076 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-121 IK4003085

Alarm	Attributes	Applicable major release
Name: IK4003085 (3985) Type: equipmentAlarm Package: lte.IK4003085 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB ALL MODEM CELL RESOURCES FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates all modem physical cell failure.		
Remedial action: Reset the BB.		

Table 29-122 IK4003103

Alarm	Attributes	Applicable major release
Name: IK4003103 (5200) Type: communicationsAlarm Package: lte.IK4003103 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB CELL RESOURCES NOT ALLOCATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the BB requested more HSIQ links than free HSIQ links available at CB level.		
Remedial action: This alarm can be raised transiently in eCCM+3bCEM configurations. eNB will automatically solve it. If, the problem persists, reset the BB.		

Table 29-123 IK4003104

Alarm	Attributes	Applicable major release
Name: IK4003104 (7963) Type: equipmentAlarm Package: lte.IK4003104 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE1 FAILURE DUE TO LOSS OF HS DATA LINK Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB slice 1 failure.		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-124 IK4003105

Alarm	Attributes	Applicable major release
Name: IK4003105 (7964) Type: equipmentAlarm Package: lte.IK4003105 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE2 FAILURE DUE TO LOSS OF HS DATA LINK Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB slice 2 failure.		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-125 IK4003106

Alarm	Attributes	Applicable major release
Name: IK4003106 (7965) Type: equipmentAlarm Package: lte.IK4003106 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE3 FAILURE DUE TO LOSS OF HS DATA LINK Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB Slice 3 failure		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-126 IK4003107

Alarm	Attributes	Applicable major release
Name: IK4003107 (7966) Type: equipmentAlarm Package: lte.IK4003107 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TEMPERATURE SENSOR FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-126 IK4003107 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a temperature sensor failure.		
Remedial action: Reset the BB in low traffic hours,if problem persists then replace the BB		

Table 29-127 IK4003108

Alarm	Attributes	Applicable major release
Name: IK4003108 (8518) Type: equipmentAlarm Package: lte.IK4003108 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-128 IK4003109

Alarm	Attributes	Applicable major release
Name: IK4003109 (8519) Type: equipmentAlarm Package: lte.IK4003109 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-129 IK4003110

Alarm	Attributes	Applicable major release
Name: IK4003110 (8520) Type: equipmentAlarm Package: lte.IK4003110 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-130 IK4003111

Alarm	Attributes	Applicable major release
Name: IK4003111 (8521) Type: equipmentAlarm Package: lte.IK4003111 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB FAULT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-131 IK4003114

Alarm	Attributes	Applicable major release
Name: IK4003114 (8522) Type: equipmentAlarm Package: lte.IK4003114 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB FAILURE DUE TO LOSS OF HS DATA LINK Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB failure.		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-132 IK4003115

Alarm	Attributes	Applicable major release
Name: IK4003115 (8523) Type: equipmentAlarm Package: lte.IK4003115 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: L2 HARDWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a hardware failure on the BB.		
Remedial action: Reset the BB, replace the BB if problem persists.		

Table 29-133 IK4003117

Alarm	Attributes	Applicable major release
Name: IK4003117 (8524) Type: processingErrorAlarm Package: lte.IK4003117 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: L2 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on the BB.		

Table 29-133 IK4003117 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset BB in low traffic hours.		

Table 29-134 IK4003126

Alarm	Attributes	Applicable major release
Name: IK4003126 (8525) Type: equipmentAlarm Package: lte.IK4003126 Raised on classes: • lte.RFM • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.AMR	Severity: critical Specific problem: INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the module initialization failure.		
Remedial action: Reset the module. Use the reset command on the SAM, or reset using the remote connection to NEM. If the alarm persists, replace the module.		

Table 29-135 IK4003127

Alarm	Attributes	Applicable major release
Name: IK4003127 (8526) Type: equipmentAlarm Package: lte.IK4003127 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RetAldEntry • lte.BBCardSpecifics • lte.MODULE • lte.TmaAldEntry	Severity: major Specific problem: INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a failure of the board has been detected that cannot described by any specific alarm.		
Remedial action: The unit is automatically reset to attempt to clear the fault. If the problem persists then replace the failed board.		

Table 29-136 IK4003128

Alarm	Attributes	Applicable major release
Name: IK4003128 (8527) Type: processingErrorAlarm Package: lte.IK4003128 Raised on classes: • lte.RFME • lte.BBCardSpecifics	Severity: minor Specific problem: FAULT DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software download failure.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-137 IK4003129

Alarm	Attributes	Applicable major release
Name: IK4003129 (8528) Type: equipmentAlarm Package: lte.IK4003129 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: OVER TEMP MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the unit's temperature is rising to the shutdown limit.		
Remedial action: Check for additional fan or air filter alarms. Check for proper fan operation and that the fan type is compatible with the system configuration, check that system inlet temperature is within operating range.		

Table 29-138 IK4003130

Alarm	Attributes	Applicable major release
Name: IK4003130 (8529) Type: equipmentAlarm Package: lte.IK4003130 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: critical Specific problem: OVER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the unit's temperature is above operating range.		
Remedial action: Check for additional fan or air filter alarms. Check for proper fan operation and that the fan type is compatible with the system configuration, check that system inlet temperature is within operating range.		

Table 29-139 IK4003131

Alarm	Attributes	Applicable major release
Name: IK4003131 (8530) Type: processingErrorAlarm Package: lte.IK4003131 Raised on classes: • lte.RFM • lte.RetAldEntry • lte.BBCardSpecifics • lte.Rae	Severity: critical Specific problem: SOFTWARE FAIL Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a general platform software failure.		
Remedial action: Reset the module.		

Table 29-140 IK4003132

Alarm	Attributes	Applicable major release
Name: IK4003132 (8531) Type: processingErrorAlarm Package: lte.IK4003132 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: L1 SOFTWARE FAIL Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a software failure on the module.		
Remedial action: Reset the module.		

Table 29-141 IK4003133

Alarm	Attributes	Applicable major release
Name: IK4003133 (8532) Type: equipmentAlarm Package: lte.IK4003133 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: critical Specific problem: FAILURE SLAVE SOC Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure of a Slave SOC.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. Replace the unit if the problem persists.		

Table 29-142 IK4003134

Alarm	Attributes	Applicable major release
Name: IK4003134 (8533) Type: equipmentAlarm Package: lte.IK4003134 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: critical Specific problem: CARD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a board failure in an eNodeB.		
Remedial action: The board is automatically reset to attempt to clear the fault. Replace the board if the problem persists.		

Table 29-143 IK4003138

Alarm	Attributes	Applicable major release
Name: IK4003138 (8534) Type: equipmentAlarm Package: lte.IK4003138 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: critical Specific problem: MODEM CELL RESOURCES FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-144 IK4003139

Alarm	Attributes	Applicable major release
Name: IK4003139 (8535) Type: processingErrorAlarm Package: lte.IK4003139 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: L2 SOFTWARE FAIL Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a software failure on the board.		
Remedial action: Reset the board.		

Table 29-145 IK4003142

Alarm	Attributes	Applicable major release
Name: IK4003142 (8536) Type: processingErrorAlarm Package: lte.IK4003142 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 1-3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-146 IK4003143

Alarm	Attributes	Applicable major release
Name: IK4003143 (8537) Type: processingErrorAlarm Package: lte.IK4003143 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 1-3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB unit.		
Remedial action: No action is required.		

Table 29-147 IK4003144

Alarm	Attributes	Applicable major release
Name: IK4003144 (8538) Type: processingErrorAlarm Package: lte.IK4003144 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 1-3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-148 IK4003146

Alarm	Attributes	Applicable major release
Name: IK4003146 (8539) Type: equipmentAlarm Package: lte.IK4003146 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE1 FAILURE DUE TO LOSS OF HS DATA LINK SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-148 IK4003146 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a failure of the BB to CB link, which leads to BB slice 1 failure.		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-149 IK4003147

Alarm	Attributes	Applicable major release
Name: IK4003147 (8540) Type: equipmentAlarm Package: lte.IK4003147 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE2 FAILURE DUE TO LOSS OF HS DATA LINK SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB slice 2 failure.		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-150 IK4003148

Alarm	Attributes	Applicable major release
Name: IK4003148 (8541) Type: equipmentAlarm Package: lte.IK4003148 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB SLICE3 FAILURE DUE TO LOSS OF HS DATA LINK SOC-SLICE 1-3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure of the BB to CB link, which leads to BB Slice 3 failure		
Remedial action: Reset BB, reset eNodeB, replace BB or CB if problem persists.		

Table 29-151 IK4003149

Alarm	Attributes	Applicable major release
Name: IK4003149 (10046) Type: equipmentAlarm Package: lte.IK4003149 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: MODEM RESET REQUIRED DUE TO RE-ASSIGNMENT OF MODEM RESOURCES Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: The alarm indicates that a Modem needs to be reset to take into account re-assignment of its resources to cells.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-152 IK4003153

Alarm	Attributes	Applicable major release
Name: IK4003153 (10047) Type: processingErrorAlarm Package: lte.IK4003153 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: warning Specific problem: L1 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a software warning on a CB or BB SOC unit.		
Remedial action: No action is required.		

Table 29-153 IK4003154

Alarm	Attributes	Applicable major release
Name: IK4003154 (10048) Type: processingErrorAlarm Package: lte.IK4003154 Raised on classes: • lte.BBCardSpecifics • lte.MODULE	Severity: warning Specific problem: L2 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a software warning on the BB/CB/SCB.		
Remedial action: Reset BB/CB/SCB in low traffic hours.		

Table 29-154 IK4004001

Alarm	Attributes	Applicable major release
Name: IK4004001 (2184) Type: equipmentAlarm Package: lte.IK4004001 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to initialize the associated resources.		
Remedial action: Reset eNodeB. If the alarm persists, replace the CB.		

Table 29-155 IK4004002

Alarm	Attributes	Applicable major release
Name: IK4004002 (2185) Type: equipmentAlarm Package: lte.IK4004002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB OSC LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a hardware failure of the oscillator.		
Remedial action: If the alarm persists for more than a minute, replace the CB.		

Table 29-156 IK4004003

Alarm	Attributes	Applicable major release
Name: IK4004003 (5201) Type: equipmentAlarm Package: lte.IK4004003 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB 1PPS AND TOD REF INPUT LOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the loss of the Ingress Reference 1PPS signal.		
Remedial action: Check the 1PPS+ToD External Reference Connectivity. If fault persist, call next level of support		

Table 29-157 IK4004004

Alarm	Attributes	Applicable major release
Name: IK4004004 (5202) Type: equipmentAlarm Package: lte.IK4004004 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB 1PPS AND TOD REF INPUT PROTOCOL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the Failure of the Ingress 1PPS+ToD Protocol Link.		
Remedial action: Check the 1PPS+ToD External Reference Connectivity. If fault persist, call next level of support		

Table 29-158 IK4004005

Alarm	Attributes	Applicable major release
Name: IK4004005 (5203) Type: equipmentAlarm Package: lte.IK4004005 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-158 IK4004005 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that a failure of the controller board has been detected that cannot described by any specific alarm.		
Remedial action: Reset the unit manually to attempt to clear the fault If the problem persists then replace the controller board.		

Table 29-159 IK4004006

Alarm	Attributes	Applicable major release
Name: IK4004006 (5204) Type: equipmentAlarm Package: lte.IK4004006 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB OSC I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot tune the OSC		
Remedial action: Reset the eNodeB or replace the OSC		

Table 29-160 IK4004007

Alarm	Attributes	Applicable major release
Name: IK4004007 (5205) Type: equipmentAlarm Package: lte.IK4004007 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB OSC OUT OF TUNE RANGE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The OSC is close to its life cycle		
Remedial action: Replace the OSC		

Table 29-161 IK4004008

Alarm	Attributes	Applicable major release
Name: IK4004008 (5206) Type: equipmentAlarm Package: lte.IK4004008 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 4 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-162 IK4004009

Alarm	Attributes	Applicable major release
Name: IK4004009 (2186) Type: equipmentAlarm Package: lte.IK4004009 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB FILE SYSTEM ACCESS FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to access files in a partition of the CB file system.		
Remedial action: Reset the eNodeB. If the alarm persists, replace the CB.		

Table 29-163 IK4004011

Alarm	Attributes	Applicable major release
Name: IK4004011 (2187) Type: equipmentAlarm Package: lte.IK4004011 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB FLYWHEEL CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for too long and timing may have drifted enough to cause RF violations.		
Remedial action: Check for reference source alarms: GPS RECEIVER (4004083);GPS 1PPS LOSS (4004065);LOSS OF SYNCE (4004160);PTP LOSS OF PRIMARY SYNC(4004162)		

Table 29-164 IK4004012

Alarm	Attributes	Applicable major release
Name: IK4004012 (2188) Type: equipmentAlarm Package: lte.IK4004012 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB FLYWHEEL MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for an extended time and timing may have drifted enough.		
Remedial action: Check for reference source alarms: GPS RECEIVER (4004083);GPS 1PPS LOSS (4004065);LOSS OF SYNCE (4004160);PTP LOSS OF PRIMARY SYNC(4004162)		

Table 29-165 IK4004013

Alarm	Attributes	Applicable major release
Name: IK4004013 (2189) Type: equipmentAlarm Package: lte.IK4004013 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FLYWHEEL MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for an extended time and timing may have drifted enough.		
Remedial action: Check for reference source alarms: GPS RECEIVER (4004083);GPS 1PPS LOSS (4004065);LOSS OF SYNCE (4004160);PTP LOSS OF PRIMARY SYNC(4004162)		

Table 29-166 IK4004014

Alarm	Attributes	Applicable major release
Name: IK4004014 (2190) Type: equipmentAlarm Package: lte.IK4004014 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB FLYWHEEL START Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The timing reference source (e.g., GPS or 1588) is not available.		
Remedial action: Check for reference source alarms: GPS RECEIVER (4004083);GPS 1PPS LOSS (4004065);LOSS OF SYNCE (4004160);PTP LOSS OF PRIMARY SYNC(4004162)		

Table 29-167 IK4004018

Alarm	Attributes	Applicable major release
Name: IK4004018 (2194) Type: equipmentAlarm Package: lte.IK4004018 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-168 IK4004019

Alarm	Attributes	Applicable major release
Name: IK4004019 (2195) Type: equipmentAlarm Package: lte.IK4004019 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-168 IK4004019 (continued)

Alarm	Attributes	Applicable major release
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-169 IK4004020

Alarm	Attributes	Applicable major release
Name: IK4004020 (2196) Type: equipmentAlarm Package: lte.IK4004020 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-170 IK4004021

Alarm	Attributes	Applicable major release
Name: IK4004021 (2197) Type: equipmentAlarm Package: lte.IK4004021 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-171 IK4004022

Alarm	Attributes	Applicable major release
Name: IK4004022 (2198) Type: equipmentAlarm Package: lte.IK4004022 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-172 IK4004023

Alarm	Attributes	Applicable major release
Name: IK4004023 (2199) Type: equipmentAlarm Package: lte.IK4004023 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-173 IK4004024

Alarm	Attributes	Applicable major release
Name: IK4004024 (2200) Type: equipmentAlarm Package: lte.IK4004024 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-174 IK4004025

Alarm	Attributes	Applicable major release
Name: IK4004025 (2201) Type: equipmentAlarm Package: lte.IK4004025 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-175 IK4004026

Alarm	Attributes	Applicable major release
Name: IK4004026 (2202) Type: equipmentAlarm Package: lte.IK4004026 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		

Table 29-175 IK4004026 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-176 IK4004027

Alarm	Attributes	Applicable major release
Name: IK4004027 (2203) Type: equipmentAlarm Package: lte.IK4004027 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-177 IK4004028

Alarm	Attributes	Applicable major release
Name: IK4004028 (2204) Type: equipmentAlarm Package: lte.IK4004028 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-178 IK4004029

Alarm	Attributes	Applicable major release
Name: IK4004029 (2205) Type: equipmentAlarm Package: lte.IK4004029 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-179 IK4004030

Alarm	Attributes	Applicable major release
Name: IK4004030 (2206) Type: equipmentAlarm Package: lte.IK4004030 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-180 IK4004031

Alarm	Attributes	Applicable major release
Name: IK4004031 (2207) Type: equipmentAlarm Package: lte.IK4004031 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-181 IK4004032

Alarm	Attributes	Applicable major release
Name: IK4004032 (2208) Type: equipmentAlarm Package: lte.IK4004032 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-182 IK4004033

Alarm	Attributes	Applicable major release
Name: IK4004033 (2209) Type: equipmentAlarm Package: lte.IK4004033 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-183 IK4004034

Alarm	Attributes	Applicable major release
Name: IK4004034 (2210) Type: equipmentAlarm Package: lte.IK4004034 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-184 IK4004035

Alarm	Attributes	Applicable major release
Name: IK4004035 (2211) Type: equipmentAlarm Package: lte.IK4004035 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-185 IK4004036

Alarm	Attributes	Applicable major release
Name: IK4004036 (2212) Type: equipmentAlarm Package: lte.IK4004036 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-186 IK4004037

Alarm	Attributes	Applicable major release
Name: IK4004037 (2213) Type: equipmentAlarm Package: lte.IK4004037 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		

Table 29-186 IK4004037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace the SFP for this port.		

Table 29-187 IK4004038

Alarm	Attributes	Applicable major release
Name: IK4004038 (2214) Type: equipmentAlarm Package: lte.IK4004038 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-188 IK4004039

Alarm	Attributes	Applicable major release
Name: IK4004039 (2215) Type: equipmentAlarm Package: lte.IK4004039 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-189 IK4004040

Alarm	Attributes	Applicable major release
Name: IK4004040 (2216) Type: equipmentAlarm Package: lte.IK4004040 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-190 IK4004041

Alarm	Attributes	Applicable major release
Name: IK4004041 (2217) Type: equipmentAlarm Package: lte.IK4004041 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-191 IK4004042

Alarm	Attributes	Applicable major release
Name: IK4004042 (2218) Type: equipmentAlarm Package: lte.IK4004042 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-192 IK4004043

Alarm	Attributes	Applicable major release
Name: IK4004043 (2219) Type: equipmentAlarm Package: lte.IK4004043 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-193 IK4004044

Alarm	Attributes	Applicable major release
Name: IK4004044 (2220) Type: equipmentAlarm Package: lte.IK4004044 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-194 IK4004045

Alarm	Attributes	Applicable major release
Name: IK4004045 (2221) Type: equipmentAlarm Package: lte.IK4004045 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-195 IK4004046

Alarm	Attributes	Applicable major release
Name: IK4004046 (2222) Type: equipmentAlarm Package: lte.IK4004046 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-196 IK4004047

Alarm	Attributes	Applicable major release
Name: IK4004047 (2223) Type: equipmentAlarm Package: lte.IK4004047 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-197 IK4004054

Alarm	Attributes	Applicable major release
Name: IK4004054 (2224) Type: equipmentAlarm Package: lte.IK4004054 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-198 IK4004055

Alarm	Attributes	Applicable major release
Name: IK4004055 (2225) Type: equipmentAlarm Package: lte.IK4004055 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-199 IK4004056

Alarm	Attributes	Applicable major release
Name: IK4004056 (2226) Type: equipmentAlarm Package: lte.IK4004056 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-200 IK4004057

Alarm	Attributes	Applicable major release
Name: IK4004057 (2227) Type: equipmentAlarm Package: lte.IK4004057 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-201 IK4004058

Alarm	Attributes	Applicable major release
Name: IK4004058 (2228) Type: equipmentAlarm Package: lte.IK4004058 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-202 IK4004059

Alarm	Attributes	Applicable major release
Name: IK4004059 (2229) Type: equipmentAlarm Package: lte.IK4004059 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: One or more data channels on this CPRI have failed.		
Remedial action: Reset RFM.		

Table 29-203 IK4004061

Alarm	Attributes	Applicable major release
Name: IK4004061 (2231) Type: equipmentAlarm Package: lte.IK4004061 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB ALL CPRIPORTS FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of all CPRI ports.		
Remedial action: Reset the eNodeB. If the alarm persists, replace the CB.		

Table 29-204 IK4004065

Alarm	Attributes	Applicable major release
Name: IK4004065 (2235) Type: equipmentAlarm Package: lte.IK4004065 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB GPS 1PPS LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the loss of GPS receiver 1PPS signal.		
Remedial action: Check GPS signal, GPS antenna, external GPS receiver if present. If fault persist, call next level of support		

Table 29-205 IK4004066

Alarm	Attributes	Applicable major release
Name: IK4004066 (2236) Type: equipmentAlarm Package: lte.IK4004066 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL BHPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the received optical signal level is very low on the backhaul port.		
Remedial action: Check the CPRI cable and SFPs at CB and RFM.		

Table 29-206 IK4004067

Alarm	Attributes	Applicable major release
Name: IK4004067 (2237) Type: equipmentAlarm Package: lte.IK4004067 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL BHPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the received optical signal level is very low on the backhaul port.		
Remedial action: Check the CPRI cable and SFPs at CB and RFM.		

Table 29-207 IK4004073

Alarm	Attributes	Applicable major release
Name: IK4004073 (2239) Type: equipmentAlarm Package: lte.IK4004073 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB OSC OVER TEMP Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the CB timing oscillator temperature is above the specification limit.		
Remedial action: Check for proper fan operation and that fan is compatible with modem unit, check DBU inlet temperature is within operating range. Replace the CB if necessary.		

Table 29-208 IK4004075

Alarm	Attributes	Applicable major release
Name: IK4004075 (2241) Type: equipmentAlarm Package: lte.IK4004075 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB SYSTEM CLOCK UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the system clock is not available. The alarm is applicable for 1588 system clock, syncE, GPS and external reference sources.		
Remedial action: Check the synchronization sources and provisioning.		

Table 29-209 IK4004082

Alarm	Attributes	Applicable major release
Name: IK4004082 (2248) Type: equipmentAlarm Package: lte.IK4004082 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB GPS ANT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a GPS antenna failure.		

Table 29-209 IK4004082 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the GPS antenna.		

Table 29-210 IK4004083

Alarm	Attributes	Applicable major release
Name: IK4004083 (2249) Type: equipmentAlarm Package: lte.IK4004083 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB GPS RECEIVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The GPS receiver has failed and cannot provide a timing reference signal.		
Remedial action: Ensure that eNodeB has completed initialization. Check the cable connection to the External GPS Receiver if equipped, replace receiver if necessary. If internal receiver then replace the CB.		

Table 29-211 IK4004091

Alarm	Attributes	Applicable major release
Name: IK4004091 (2251) Type: equipmentAlarm Package: lte.IK4004091 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-212 IK4004092

Alarm	Attributes	Applicable major release
Name: IK4004092 (2252) Type: equipmentAlarm Package: lte.IK4004092 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-213 IK4004093

Alarm	Attributes	Applicable major release
Name: IK4004093 (2253) Type: equipmentAlarm Package: lte.IK4004093 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-214 IK4004094

Alarm	Attributes	Applicable major release
Name: IK4004094 (2254) Type: equipmentAlarm Package: lte.IK4004094 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-215 IK4004095

Alarm	Attributes	Applicable major release
Name: IK4004095 (2255) Type: equipmentAlarm Package: lte.IK4004095 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-216 IK4004096

Alarm	Attributes	Applicable major release
Name: IK4004096 (2256) Type: equipmentAlarm Package: lte.IK4004096 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-217 IK4004097

Alarm	Attributes	Applicable major release
Name: IK4004097 (2257) Type: equipmentAlarm Package: lte.IK4004097 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-218 IK4004098

Alarm	Attributes	Applicable major release
Name: IK4004098 (2258) Type: equipmentAlarm Package: lte.IK4004098 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-219 IK4004099

Alarm	Attributes	Applicable major release
Name: IK4004099 (2259) Type: equipmentAlarm Package: lte.IK4004099 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-220 IK4004100

Alarm	Attributes	Applicable major release
Name: IK4004100 (2260) Type: equipmentAlarm Package: lte.IK4004100 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-221 IK4004101

Alarm	Attributes	Applicable major release
Name: IK4004101 (2261) Type: equipmentAlarm Package: lte.IK4004101 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 11 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-222 IK4004102

Alarm	Attributes	Applicable major release
Name: IK4004102 (2262) Type: equipmentAlarm Package: lte.IK4004102 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOS LOF HSIQPORT 12 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-223 IK4004104

Alarm	Attributes	Applicable major release
Name: IK4004104 (2263) Type: equipmentAlarm Package: lte.IK4004104 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB GPS RECEIVER COMM FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The CB cannot communicate with the GPS receiver.		
Remedial action: Ensure that eNodeB has completed initialization. Check the cable connection to the External GPS Receiver if equipped, replace receiver if necessary. If internal receiver then replace the CB.		

Table 29-224 IK4004107

Alarm	Attributes	Applicable major release
Name: IK4004107 (2266) Type: equipmentAlarm Package: lte.IK4004107 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L

Table 29-224 IK4004107 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-225 IK4004117

Alarm	Attributes	Applicable major release
Name: IK4004117 (2276) Type: equipmentAlarm Package: lte.IK4004117 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB OVER TEMP MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CB temperature is rising near the shutdown limit.		
Remedial action: Check for fan failure or high ambient temperature.		

Table 29-226 IK4004118

Alarm	Attributes	Applicable major release
Name: IK4004118 (2277) Type: equipmentAlarm Package: lte.IK4004118 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB OVER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CB temperature is above the operating range.		
Remedial action: CB autonomously powers down. Check for fan failure or high ambient temperature.		

Table 29-227 IK4004126

Alarm	Attributes	Applicable major release
Name: IK4004126 (2285) Type: equipmentAlarm Package: lte.IK4004126 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB FAILURE SLAVE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of a Slave SOC.		
Remedial action: Reset the eNodeB manually to attempt to clear the fault. Replace the controller board if the problem persists.		

Table 29-228 IK4004127

Alarm	Attributes	Applicable major release
Name: IK4004127 (2286) Type: equipmentAlarm Package: lte.IK4004127 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB FAILURE SLAVE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of a Slave SOC.		
Remedial action: Reset the eNodeB manually to attempt to clear the fault. Replace the controller board if the problem persists.		

Table 29-229 IK4004128

Alarm	Attributes	Applicable major release
Name: IK4004128 (2287) Type: equipmentAlarm Package: lte.IK4004128 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB CARD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of controller board.		
Remedial action: Reset the eNodeB manually to attempt to clear the fault. Replace the controller board if the problem persists		

Table 29-230 IK4004129

Alarm	Attributes	Applicable major release
Name: IK4004129 (2288) Type: equipmentAlarm Package: lte.IK4004129 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-231 IK4004130

Alarm	Attributes	Applicable major release
Name: IK4004130 (2289) Type: equipmentAlarm Package: lte.IK4004130 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP1 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 1 through I2C		

Table 29-231 IK4004130 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-232 IK4004131

Alarm	Attributes	Applicable major release
Name: IK4004131 (2290) Type: equipmentAlarm Package: lte.IK4004131 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP2 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 2 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-233 IK4004132

Alarm	Attributes	Applicable major release
Name: IK4004132 (2291) Type: equipmentAlarm Package: lte.IK4004132 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP3 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 3 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-234 IK4004133

Alarm	Attributes	Applicable major release
Name: IK4004133 (2292) Type: equipmentAlarm Package: lte.IK4004133 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP4 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 4 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-235 IK4004134

Alarm	Attributes	Applicable major release
Name: IK4004134 (2293) Type: equipmentAlarm Package: lte.IK4004134 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP5 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 5 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-236 IK4004135

Alarm	Attributes	Applicable major release
Name: IK4004135 (2294) Type: equipmentAlarm Package: lte.IK4004135 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP6 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 6 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-237 IK4004138

Alarm	Attributes	Applicable major release
Name: IK4004138 (2297) Type: equipmentAlarm Package: lte.IK4004138 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP7 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 7 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-238 IK4004139

Alarm	Attributes	Applicable major release
Name: IK4004139 (2298) Type: equipmentAlarm Package: lte.IK4004139 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP8 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP 8 through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-239 IK4004140

Alarm	Attributes	Applicable major release
Name: IK4004140 (2299) Type: equipmentAlarm Package: lte.IK4004140 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TOD OUT OF SYNC Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the GPS timing pulses may be missing or incorrect.		
Remedial action: Replace the External GPS Receiver or CB (if using internal GPS receiver).		

Table 29-240 IK4004143

Alarm	Attributes	Applicable major release
Name: IK4004143 (5207) Type: equipmentAlarm Package: lte.IK4004143 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SFP9 I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-241 IK4004144

Alarm	Attributes	Applicable major release
Name: IK4004144 (2988) Type: equipmentAlarm Package: lte.IK4004144 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-242 IK4004145

Alarm	Attributes	Applicable major release
Name: IK4004145 (2989) Type: equipmentAlarm Package: lte.IK4004145 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		

Table 29-242 IK4004145 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the additional information for maintenance action details.		

Table 29-243 IK4004146

Alarm	Attributes	Applicable major release
Name: IK4004146 (2990) Type: equipmentAlarm Package: lte.IK4004146 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-244 IK4004147

Alarm	Attributes	Applicable major release
Name: IK4004147 (2991) Type: equipmentAlarm Package: lte.IK4004147 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-245 IK4004148

Alarm	Attributes	Applicable major release
Name: IK4004148 (2992) Type: equipmentAlarm Package: lte.IK4004148 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-246 IK4004152

Alarm	Attributes	Applicable major release
Name: IK4004152 (2996) Type: equipmentAlarm Package: lte.IK4004152 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 3 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-247 IK4004154

Alarm	Attributes	Applicable major release
Name: IK4004154 (2998) Type: equipmentAlarm Package: lte.IK4004154 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB LOOPBACK INACTIVITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates there is no packet activity for the interval specified in the loopback activation.		
Remedial action: Reset the eNodeB. Call the next level of support		

Table 29-248 IK4004155

Alarm	Attributes	Applicable major release
Name: IK4004155 (3637) Type: equipmentAlarm Package: lte.IK4004155 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB PTP CLIENT INITIALIZING 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the 1588 client algorithm is stabilizing from a cold start-up, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: If alarm continues assess the Packet delay variation on the Network Interface.		

Table 29-249 IK4004156

Alarm	Attributes	Applicable major release
Name: IK4004156 (3638) Type: equipmentAlarm Package: lte.IK4004156 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB PTP CLIENT INITIALIZING 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-249 IK4004156 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the 1588 client algorithm is stabilizing from a cold start-up, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: If alarm continues assess the Packet delay variation on the Network Interface.		

Table 29-250 IK4004157

Alarm	Attributes	Applicable major release
Name: IK4004157 (3639) Type: equipmentAlarm Package: lte.IK4004157 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB GPS LOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that GPS satellite lock has been lost after timing has been synchronized.		
Remedial action: Check the GPS antenna placement, GPS antenna status, or GPS antenna cable. Replace the External GPS Receiver or CB (if using internal GPS receiver).		

Table 29-251 IK4004158

Alarm	Attributes	Applicable major release
Name: IK4004158 (3640) Type: equipmentAlarm Package: lte.IK4004158 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB OSC IN WARMUP Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the CB timing oscillator is below its operating temperature range.		
Remedial action: Wait for the oscillator module to warm up, worst case delay is 12 minutes at -5 Degree C cold start.. If the alarm persists and ambient temperature is within normal operating range then replace the CB.		

Table 29-252 IK4004159

Alarm	Attributes	Applicable major release
Name: IK4004159 (3641) Type: equipmentAlarm Package: lte.IK4004159 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOSS OF PRIMARY REFERENCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the primary reference source is not available.		
Remedial action: Check the primary reference source.		

Table 29-253 IK4004160

Alarm	Attributes	Applicable major release
Name: IK4004160 (3642) Type: equipmentAlarm Package: lte.IK4004160 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB LOSS OF SYNCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The SyncE timing reference is not available.		
Remedial action: The Backhaul Node connecting to the eNB cannot supply an accurate Synchronous Ethernet clock. Check the clock source on this Backhaul Node.		

Table 29-254 IK4004162

Alarm	Attributes	Applicable major release
Name: IK4004162 (3644) Type: equipmentAlarm Package: lte.IK4004162 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB PTP LOSS OF PRIMARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of synchronization with the primary 1588 grandmaster server, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: Check configuration of link to 1588 Grandmaster is correct.\nIf problem persists check the packet delay variation on the eNb backhaul interface.		

Table 29-255 IK4004163

Alarm	Attributes	Applicable major release
Name: IK4004163 (3645) Type: equipmentAlarm Package: lte.IK4004163 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB PTP LOSS OF SECONDARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of synchronization with the secondary 1588 grandmaster server, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: Check configuration of link to 1588 Grandmaster is correct.\nIf problem persists check the packet delay variation on the eNb backhaul interface.		

Table 29-256 IK4004164

Alarm	Attributes	Applicable major release
Name: IK4004164 (3646) Type: equipmentAlarm Package: lte.IK4004164 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB PTP UNEXPECTED LONG INITIALIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that 1588 client has taken longer than expected to achieve complete synchronization. When the 1588 message transfer is set to Discontinuous mode and the , this alarm indicates lock has not been obtained in a message transfer session before the next timed session, when the session length is defined by gaining Lock.		
Remedial action: Verify 1588 grandmaster is operating correctly, check network conditions, otherwise reset the eNodeB. Note: if eNB has synchronized to an alternative available source, then reset of eNodeB will be service impacting.		

Table 29-257 IK4004166

Alarm	Attributes	Applicable major release
Name: IK4004166 (3648) Type: equipmentAlarm Package: lte.IK4004166 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB GPS INSUFFICIENT FIXED SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that insufficient fixed satellites are available to get GPS synchronization.		
Remedial action: Check the GPS antenna location and status. Replace GPS antenna, cable or receiver if necessary.		

Table 29-258 IK4004167

Alarm	Attributes	Applicable major release
Name: IK4004167 (3649) Type: equipmentAlarm Package: lte.IK4004167 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB GPS INSUFFICIENT VISIBLE SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that insufficient visible satellites are available to get GPS synchronization.		
Remedial action: Check the GPS antenna location and status. Replace GPS antenna, cable or receiver if necessary.		

Table 29-259 IK4004172

Alarm	Attributes	Applicable major release
Name: IK4004172 (4632) Type: equipmentAlarm Package: lte.IK4004172 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-260 IK4004173

Alarm	Attributes	Applicable major release
Name: IK4004173 (4633) Type: equipmentAlarm Package: lte.IK4004173 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-261 IK4004174

Alarm	Attributes	Applicable major release
Name: IK4004174 (4634) Type: equipmentAlarm Package: lte.IK4004174 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS LSL CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-262 IK4004175

Alarm	Attributes	Applicable major release
Name: IK4004175 (4635) Type: equipmentAlarm Package: lte.IK4004175 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-263 IK4004176

Alarm	Attributes	Applicable major release
Name: IK4004176 (4636) Type: equipmentAlarm Package: lte.IK4004176 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-264 IK4004177

Alarm	Attributes	Applicable major release
Name: IK4004177 (4637) Type: equipmentAlarm Package: lte.IK4004177 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB RAI CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The first RFM on the CPRI port is reporting a CPRI link alarm.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary. Reset eNodeB or replace CB if problem persists.		

Table 29-265 IK4004178

Alarm	Attributes	Applicable major release
Name: IK4004178 (4638) Type: equipmentAlarm Package: lte.IK4004178 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-266 IK4004179

Alarm	Attributes	Applicable major release
Name: IK4004179 (4639) Type: equipmentAlarm Package: lte.IK4004179 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		

Table 29-266 IK4004179 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-267 IK4004180

Alarm	Attributes	Applicable major release
Name: IK4004180 (4640) Type: equipmentAlarm Package: lte.IK4004180 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB LOS LOF CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (CB and RFM) for failures, otherwise reset the RFM or reset the eNodeB		

Table 29-268 IK4004181

Alarm	Attributes	Applicable major release
Name: IK4004181 (4641) Type: equipmentAlarm Package: lte.IK4004181 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-269 IK4004182

Alarm	Attributes	Applicable major release
Name: IK4004182 (4642) Type: equipmentAlarm Package: lte.IK4004182 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-270 IK4004183

Alarm	Attributes	Applicable major release
Name: IK4004183 (4643) Type: equipmentAlarm Package: lte.IK4004183 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB TRANS TX FAILURE CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the CB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-271 IK4004184

Alarm	Attributes	Applicable major release
Name: IK4004184 (4644) Type: equipmentAlarm Package: lte.IK4004184 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-272 IK4004185

Alarm	Attributes	Applicable major release
Name: IK4004185 (4645) Type: equipmentAlarm Package: lte.IK4004185 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-273 IK4004186

Alarm	Attributes	Applicable major release
Name: IK4004186 (4646) Type: equipmentAlarm Package: lte.IK4004186 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB TRANS RX LOS CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end), verify the RFM is operating.		

Table 29-274 IK4004190

Alarm	Attributes	Applicable major release
Name: IK4004190 (4647) Type: equipmentAlarm Package: lte.IK4004190 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates one or more data channels on this CPRI have failed.		
Remedial action: Reset the RFM connected to this CPRI port.		

Table 29-275 IK4004191

Alarm	Attributes	Applicable major release
Name: IK4004191 (4648) Type: equipmentAlarm Package: lte.IK4004191 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates one or more data channels on this CPRI have failed.		
Remedial action: Reset the RFM connected to this CPRI port.		

Table 29-276 IK4004192

Alarm	Attributes	Applicable major release
Name: IK4004192 (4649) Type: equipmentAlarm Package: lte.IK4004192 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB SDI CPRIPORT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates one or more data channels on this CPRI have failed.		
Remedial action: Reset the RFM connected to this CPRI port.		

Table 29-277 IK4004193

Alarm	Attributes	Applicable major release
Name: IK4004193 (5208) Type: equipmentAlarm Package: lte.IK4004193 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 5 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		

Table 29-277 IK4004193 (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operator may update the SFP on the BBU.		

Table 29-278 IK4004194

Alarm	Attributes	Applicable major release
Name: IK4004194 (5209) Type: equipmentAlarm Package: lte.IK4004194 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 6 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-279 IK4004195

Alarm	Attributes	Applicable major release
Name: IK4004195 (5210) Type: equipmentAlarm Package: lte.IK4004195 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 7 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-280 IK4004196

Alarm	Attributes	Applicable major release
Name: IK4004196 (5211) Type: equipmentAlarm Package: lte.IK4004196 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 8 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-281 IK4004197

Alarm	Attributes	Applicable major release
Name: IK4004197 (5212) Type: equipmentAlarm Package: lte.IK4004197 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB SFP INCOMPATIBILITY CPRIPORT 9 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the BBU.		

Table 29-282 IK4004198

Alarm	Attributes	Applicable major release
Name: IK4004198 (7967) Type: equipmentAlarm Package: lte.IK4004198 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: GNSS FIRMWARE UPGRADE MISMATCH Implicitly cleared: true Default probable cause: versionMismatch	Release: • LR15.1.L
Description: The GNSS firmware is incompatible with the GNSS receiver component.		
Remedial action: Check the GNSS type and ensure firmware to be downloaded is compatible with GNSS component vendor and part..		

Table 29-283 IK4004199

Alarm	Attributes	Applicable major release
Name: IK4004199 (7968) Type: equipmentAlarm Package: lte.IK4004199 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: GNSS FIRMWARE UPGRADE FAILURE Implicitly cleared: true Default probable cause: versionMismatch	Release: • LR15.1.L
Description: The GNSS firmware fails to be successfully loaded to the GNSS receiver component		
Remedial action: Check the GNSS type and ensure firmware to be downloaded is compatible with GNSS component..		

Table 29-284 IK4004200

Alarm	Attributes	Applicable major release
Name: IK4004200 (7969) Type: equipmentAlarm Package: lte.IK4004200 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB INIT GPS SELF SURVEY INPROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNB has started a high accuracy GPS survey for OTDOA, which normally takes 10 hours to complete.		
Remedial action: No action is required.		

Table 29-285 IK4004201

Alarm	Attributes	Applicable major release
Name: IK4004201 (7970) Type: equipmentAlarm Package: lte.IK4004201 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB INIT GPS SELF SURVEY FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a high accuracy GPS survey has not been successfully completed after 24 hours.		
Remedial action: Check GPS performance. Ensure good GPS receiver and GPS antenna is installed per Nokia guidelines and located to have a full sky visibility with no local interference or multipath, then power cycle the controller to restart survey. If GPS reception can't be improved then disable OTDOA (isGeoLocPhaseSyncAllowed="False), which will clear the alarm."		

Table 29-286 IK4004202

Alarm	Attributes	Applicable major release
Name: IK4004202 (8542) Type: equipmentAlarm Package: lte.IK4004202 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-287 IK4004203

Alarm	Attributes	Applicable major release
Name: IK4004203 (8543) Type: equipmentAlarm Package: lte.IK4004203 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-288 IK4004208

Alarm	Attributes	Applicable major release
Name: IK4004208 (8544) Type: processingErrorAlarm Package: lte.IK4004208 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB event detected		
Remedial action: No action is required.		

Table 29-289 IK4004209

Alarm	Attributes	Applicable major release
Name: IK4004209 (8545) Type: processingErrorAlarm Package: lte.IK4004209 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB event detected		
Remedial action: No action is required.		

Table 29-290 IK4004210

Alarm	Attributes	Applicable major release
Name: IK4004210 (8546) Type: processingErrorAlarm Package: lte.IK4004210 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-290 IK4004210 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified CB event detected		
Remedial action: No action is required.		

Table 29-291 IK4004211

Alarm	Attributes	Applicable major release
Name: IK4004211 (8547) Type: equipmentAlarm Package: lte.IK4004211 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: LOS LOF HSIQPORT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a loss of signal between BB and CB.		
Remedial action: Replace the BB if a single port fault is present. If link faults exist across multiple ports then replace the CB.		

Table 29-292 IK4004213

Alarm	Attributes	Applicable major release
Name: IK4004213 (8548) Type: processingErrorAlarm Package: lte.IK4004213 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: warning Specific problem: L1 SOFTWARE WARNING Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-293 IK4004222

Alarm	Attributes	Applicable major release
Name: IK4004222 (8549) Type: equipmentAlarm Package: lte.IK4004222 Raised on class: lte.SFP	Severity: minor Specific problem: SFP I2C FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates CB cannot read info of SFP through I2C		
Remedial action: Reset the eNodeB or replace the SFP		

Table 29-294 IK4004224

Alarm	Attributes	Applicable major release
Name: IK4004224 (8550) Type: equipmentAlarm Package: lte.IK4004224 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: OSC LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a hardware failure of the oscillator.		
Remedial action: If the alarm persists for more than a minute, replace the CB.		

Table 29-295 IK4004225

Alarm	Attributes	Applicable major release
Name: IK4004225 (8551) Type: equipmentAlarm Package: lte.IK4004225 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: FILE SYSTEM ACCESS FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to access files in a partition of the CB file system.		
Remedial action: Reset the eNodeB. If the alarm persists, replace the CB.		

Table 29-296 IK4004226

Alarm	Attributes	Applicable major release
Name: IK4004226 (8552) Type: equipmentAlarm Package: lte.IK4004226 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: FLYWHEEL START Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The timing reference source (e.g., GPS or 1588) is not available.		
Remedial action: Check for reference source alarms: GPS RECEIVER; GPS 1PPS LOSS ;LOSS OF SYNCE ;PTP LOSS OF PRIMARY SYNC		

Table 29-297 IK4004227

Alarm	Attributes	Applicable major release
Name: IK4004227 (8553) Type: equipmentAlarm Package: lte.IK4004227 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: FLYWHEEL MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for an extended time and timing may have drifted enough.		
Remedial action: Check for reference source alarms: GPS RECEIVER; GPS 1PPS LOSS ;LOSS OF SYNCE ;PTP LOSS OF PRIMARY SYNC		

Table 29-298 IK4004228

Alarm	Attributes	Applicable major release
Name: IK4004228 (8554) Type: equipmentAlarm Package: lte.IK4004228 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: FLYWHEEL MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for an extended time and timing may have drifted enough.		
Remedial action: Check for reference source alarms: GPS RECEIVER; GPS 1PPS LOSS ;LOSS OF SYNCE ;PTP LOSS OF PRIMARY SYNC		

Table 29-299 IK4004229

Alarm	Attributes	Applicable major release
Name: IK4004229 (8555) Type: equipmentAlarm Package: lte.IK4004229 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: FLYWHEEL CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The timing reference source (e.g., GPS or 1588) has been unavailable for too long and timing may have drifted enough to cause RF violations.		
Remedial action: Check for reference source alarms: GPS RECEIVER; GPS 1PPS LOSS ;LOSS OF SYNCE ;PTP LOSS OF PRIMARY SYNC		

Table 29-300 IK4004230

Alarm	Attributes	Applicable major release
Name: IK4004230 (8556) Type: equipmentAlarm Package: lte.IK4004230 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: critical Specific problem: ALL CPRIPORTS FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of all CPRI ports.		
Remedial action: Reset the eNodeB. If the alarm persists, replace the alarmed unit.		

Table 29-301 IK4004231

Alarm	Attributes	Applicable major release
Name: IK4004231 (8557) Type: equipmentAlarm Package: lte.IK4004231 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: GPS 1PPS LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the loss of GPS receiver 1PPS signal.		
Remedial action: Check GPS signal, GPS antenna, external GPS receiver if present. If fault persist, call next level of support		

Table 29-302 IK4004232

Alarm	Attributes	Applicable major release
Name: IK4004232 (8558) Type: equipmentAlarm Package: lte.IK4004232 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: SYSTEM CLOCK UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the system clock is not available. The alarm is applicable for 1588 system clock, syncE, GPS and external reference sources.		
Remedial action: Check the synchronization sources and provisioning.		

Table 29-303 IK4004233

Alarm	Attributes	Applicable major release
Name: IK4004233 (8559) Type: equipmentAlarm Package: lte.IK4004233 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: GPS ANT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a GPS antenna failure.		
Remedial action: Check the GPS antenna.		

Table 29-304 IK4004234

Alarm	Attributes	Applicable major release
Name: IK4004234 (8560) Type: equipmentAlarm Package: lte.IK4004234 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: GPS RECEIVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The GPS receiver has failed and cannot provide a timing reference signal.		
Remedial action: Ensure that eNodeB has completed initialization. Check the cable connection to the External GPS Receiver if equipped, replace receiver if necessary. If internal receiver then replace the CB.		

Table 29-305 IK4004235

Alarm	Attributes	Applicable major release
Name: IK4004235 (8561) Type: equipmentAlarm Package: lte.IK4004235 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: GPS RECEIVER COMM FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The CB cannot communicate with the GPS receiver.		
Remedial action: Ensure that eNodeB has completed initialization. Check the cable connection to the External GPS Receiver if equipped, replace receiver if necessary. If internal receiver then replace the CB.		

Table 29-306 IK4004237

Alarm	Attributes	Applicable major release
Name: IK4004237 (8562) Type: equipmentAlarm Package: lte.IK4004237 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: LOOPBACK INACTIVITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates there is no packet activity for the interval specified in the loopback activation.		
Remedial action: Reset the eNodeB. Call the next level of support		

Table 29-307 IK4004238

Alarm	Attributes	Applicable major release
Name: IK4004238 (8563) Type: equipmentAlarm Package: lte.IK4004238 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: PTP CLIENT INITIALIZING 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the 1588 client algorithm is stabilizing from a cold start-up, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: If alarm continues assess the Packet delay variation on the Network Interface.		

Table 29-308 IK4004239

Alarm	Attributes	Applicable major release
Name: IK4004239 (8564) Type: equipmentAlarm Package: lte.IK4004239 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: PTP CLIENT INITIALIZING 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the 1588 client algorithm is stabilizing from a cold start-up, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: If alarm continues assess the Packet delay variation on the Network Interface.		

Table 29-309 IK4004240

Alarm	Attributes	Applicable major release
Name: IK4004240 (8565) Type: equipmentAlarm Package: lte.IK4004240 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: GPS LOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that GPS satellite lock has been lost after timing has been synchronized.		
Remedial action: Check the GPS antenna placement, GPS antenna status, or GPS antenna cable. Replace the External GPS Receiver or CB (if using internal GPS receiver).		

Table 29-310 IK4004241

Alarm	Attributes	Applicable major release
Name: IK4004241 (8566) Type: equipmentAlarm Package: lte.IK4004241 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: LOSS OF PRIMARY REFERENCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the primary reference source is not available.		
Remedial action: Check the primary reference source.		

Table 29-311 IK4004242

Alarm	Attributes	Applicable major release
Name: IK4004242 (8567) Type: equipmentAlarm Package: lte.IK4004242 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: LOSS OF SYNCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The SyncE timing reference is not available.		
Remedial action: The Backhaul Node connecting to the eNB cannot supply an accurate Synchronous Ethernet clock. Check the clock source on this Backhaul Node.		

Table 29-312 IK4004243

Alarm	Attributes	Applicable major release
Name: IK4004243 (8568) Type: equipmentAlarm Package: lte.IK4004243 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: PTP LOSS OF PRIMARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of synchronization with the primary 1588 grandmaster server, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: Check configuration of link to 1588 Grandmaster is correct.\nIf problem persists check the packet delay variation on the eNb backhaul interface.		

Table 29-313 IK4004244

Alarm	Attributes	Applicable major release
Name: IK4004244 (8569) Type: equipmentAlarm Package: lte.IK4004244 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: PTP LOSS OF SECONDARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of synchronization with the secondary 1588 grandmaster server, when the 1588 message transfer is set to Continuous mode. This alarm is inhibited when the 1588 message transfer is in Discontinuous mode.		
Remedial action: Check configuration of link to 1588 Grandmaster is correct.\nIf problem persists check the packet delay variation on the eNb backhaul interface.		

Table 29-314 IK4004245

Alarm	Attributes	Applicable major release
Name: IK4004245 (8570) Type: equipmentAlarm Package: lte.IK4004245 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: GPS INSUFFICIENT FIXED SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that insufficient fixed satellites are available to get GPS synchronization.		
Remedial action: Check the GPS antenna location and status. Replace GPS antenna, cable or receiver if necessary.		

Table 29-315 IK4004246

Alarm	Attributes	Applicable major release
Name: IK4004246 (8571) Type: equipmentAlarm Package: lte.IK4004246 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: GPS INSUFFICIENT VISIBLE SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that insufficient visible satellites are available to get GPS synchronization.		
Remedial action: Check the GPS antenna location and status. Replace GPS antenna, cable or receiver if necessary.		

Table 29-316 IK4004248

Alarm	Attributes	Applicable major release
Name: IK4004248 (8572) Type: equipmentAlarm Package: lte.IK4004248 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: INIT GPS SELF SURVEY FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a high accuracy GPS survey has not been successfully completed after 24 hours.		
Remedial action: Check GPS performance. Ensure good GPS receiver and GPS antenna is installed per Nokia guidelines and located to have a full sky visibility with no local interference or multipath, then power cycle the controller to restart survey. If GPS reception can't be improved then disable OTDOA (isGeoLocPhaseSyncAllowed="False), which will clear the alarm."		

Table 29-317 IK4004250

Alarm	Attributes	Applicable major release
Name: IK4004250 (8573) Type: equipmentAlarm Package: lte.IK4004250 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: PTP UNEXPECTED LONG INITIALIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that 1588 client has taken longer than expected to achieve complete synchronization. When the 1588 message transfer is set to Discontinuous mode and the , this alarm indicates lock has not been obtained in a message transfer session before the next timed session, when the session length is defined by gaining Lock.		
Remedial action: Verify 1588 grandmaster is operating correctly, check network conditions, otherwise reset the eNodeB. Note: if eNB has synchronized to an alternative available source, then reset of eNodeB will be service impacting.		

Table 29-318 IK4004251

Alarm	Attributes	Applicable major release
Name: IK4004251 (8574) Type: equipmentAlarm Package: lte.IK4004251 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: INIT GPS SELF SURVEY INPROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNB has started a high accuracy GPS survey for OTDOA, which normally takes 10 hours to complete.		
Remedial action: No action is required.		

Table 29-319 IK4004256

Alarm	Attributes	Applicable major release
Name: IK4004256 (8575) Type: equipmentAlarm Package: lte.IK4004256 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: major Specific problem: BOOT/USB FLASH MISMATCH Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Uboot version in boot-flash doesn't match that in USB flash.		
Remedial action: Initiate SW download if code server path is still valid. \n If the alarms persists, manually download the correct version and reset the impacted module to switch the newly downloaded version.		

Table 29-320 IK4004257

Alarm	Attributes	Applicable major release
Name: IK4004257 (10049) Type: processingErrorAlarm Package: lte.IK4004257 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB FAULT 8 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-321 IK4004259

Alarm	Attributes	Applicable major release
Name: IK4004259 (10051) Type: equipmentAlarm Package: lte.IK4004259 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: major Specific problem: SRIO PORT WRONG CABLING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates the board is not correctly cabled to the right SRIO port of the SRIO Switch Box, according to the I&C ShelfID parameter.\n.		
Remedial action: Check the cabling of the eNB with the SRIO Switch Box, check the I&C parameter Shelf ID, check if the eNB has been reset after the I&C parameter Shelf ID has been set.\nFix the issue, and resets the eNB.		

Table 29-322 IK4004260

Alarm	Attributes	Applicable major release
Name: IK4004260 (10052) Type: equipmentAlarm Package: lte.IK4004260 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: major Specific problem: SRIO PORT FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only.\nIt indicates the opening or configuration of the SRIO port on the faceplate of the board has failed.		
Remedial action: Check the I&C parameter HotelConfig, check if the eNB has been reset after the I&C parameter HotelConfig has been set.\nFix the issue, and resets the eNB.		

Table 29-323 IK4004263

Alarm	Attributes	Applicable major release
Name: IK4004263 (11003) Type: equipmentAlarm Package: lte.IK4004263 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: major Specific problem: BOARD RESET REQUIRED DUE TO PROFILE ASSIGNMENT Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: The alarm indicates that a board needs to be reset to take into account the change of the global profile assigned to the board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the fault persists, then reset the appropriate board.		

Table 29-324 IK4004264

Alarm	Attributes	Applicable major release
Name: IK4004264 (11004) Type: equipmentAlarm Package: lte.IK4004264 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: OSC AGING MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: A problem has been detected with the hardware oscillator on the controller of the eNodeB. Because of aging effects, the oscillator is near to its operating limits.		
Remedial action: Plan for a hardware replacement in the near future.		

Table 29-325 IK4004265

Alarm	Attributes	Applicable major release
Name: IK4004265 (11005) Type: equipmentAlarm Package: lte.IK4004265 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: OSC AGING MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: A problem has been detected with the hardware oscillator on the controller of the eNodeB. Because of aging effects, the oscillator has reached its operating limits and may fail shortly.		
Remedial action: Trigger a hardware replacement.		

Table 29-326 IK4004267

Alarm	Attributes	Applicable major release
Name: IK4004267 (11006) Type: equipmentAlarm Package: lte.IK4004267 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: UNDER TEMP MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the unit's temperature is at or below the minimum recommended operating temperature.		
Remedial action: No action is required.		

Table 29-327 IK4004272

Alarm	Attributes	Applicable major release
Name: IK4004272 (11007) Type: equipmentAlarm Package: lte.IK4004272 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: 1588V2 SYNCHRONIZATION SOURCE OUT OF RANGE Implicitly cleared: true Default probable cause: timingProblem	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicated that the backhaul is not good enough to support PTP in the goal to maintain eNB frequency synchronization within the 50 ppb accuracy at the antenna interface The eNB enters Flywheeling phase, where the clock is out-of-spec		
Remedial action: Resolve faulty 1588v2 clock reference		

Table 29-328 IK4005001

Alarm	Attributes	Applicable major release
Name: IK4005001 (2300) Type: equipmentAlarm Package: lte.IK4005001 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: DBU INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to initialize the associated resources.		
Remedial action: Reset eNodeB. Check BIST result. If the alarm persists, replace the CB.		

Table 29-329 IK4005002

Alarm	Attributes	Applicable major release
Name: IK4005002 (2301) Type: equipmentAlarm Package: lte.IK4005002 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: RECTIFIER FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the rectifier has failed.		
Remedial action: Check rectifier for root cause and either replace rectifier or repair if possible.		

Table 29-330 IK4005003

Alarm	Attributes	Applicable major release
Name: IK4005003 (2302) Type: equipmentAlarm Package: lte.IK4005003 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU MEMORY ACCESS FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to access the EEPROM on the eNodeB.		

Table 29-330 IK4005003 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Call the next level of support.		

Table 29-331 IK4005004

Alarm	Attributes	Applicable major release
Name: IK4005004 (2303) Type: equipmentAlarm Package: lte.IK4005004 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to read the manufacturer data.		
Remedial action: Call the next level of support.		

Table 29-332 IK4005005

Alarm	Attributes	Applicable major release
Name: IK4005005 (5213) Type: equipmentAlarm Package: lte.IK4005005 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: BATTERY FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Battery failure (high temperature, voltage imbalance)		
Remedial action: Replace batteries.		

Table 29-333 IK4005006

Alarm	Attributes	Applicable major release
Name: IK4005006 (2304) Type: equipmentAlarm Package: lte.IK4005006 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: POWER CONTROL BOARD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that AC/DC power system control board is in failure		
Remedial action: Check power system control module. Replace power system control module.		

Table 29-334 IK4005007

Alarm	Attributes	Applicable major release
Name: IK4005007 (2305) Type: equipmentAlarm Package: lte.IK4005007 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: AC CIRCUIT BREAKER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that one or several AC breakers have tripped. May be associated to AC Main alarm.		
Remedial action: Visit basestation and check AC main supply.		

Table 29-335 IK4005008

Alarm	Attributes	Applicable major release
Name: IK4005008 (2306) Type: equipmentAlarm Package: lte.IK4005008 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: DBU INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a failure of the shelf hardware has been detected that cannot described by any specific alarm.		
Remedial action: Inspect the shelf hardware (fan unit, power converter unit, etc.), replace any faulty unit.		

Table 29-336 IK4005009

Alarm	Attributes	Applicable major release
Name: IK4005009 (2307) Type: equipmentAlarm Package: lte.IK4005009 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: FRESH AIR FILTER 1 FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that Fresh air filter 1 is clogged		
Remedial action: Replace filter.		

Table 29-337 IK4005010

Alarm	Attributes	Applicable major release
Name: IK4005010 (2308) Type: equipmentAlarm Package: lte.IK4005010 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: FRESH AIR FILTER 2 FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that Fresh air filter 2 is clogged.		

Table 29-337 IK4005010 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Replace filter.		

Table 29-338 IK4005038

Alarm	Attributes	Applicable major release
Name: IK4005038 (2336) Type: equipmentAlarm Package: lte.IK4005038 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU AC MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of multiple rectifier components.		
Remedial action: Replace the failed rectifier component.		

Table 29-339 IK4005039

Alarm	Attributes	Applicable major release
Name: IK4005039 (2337) Type: equipmentAlarm Package: lte.IK4005039 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU AC MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a minor failure in the DC rectifier unit.		
Remedial action: Replace the failed fan or the rectifier component.		

Table 29-340 IK4005040

Alarm	Attributes	Applicable major release
Name: IK4005040 (2338) Type: equipmentAlarm Package: lte.IK4005040 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU AC INPUT OUT OF SPEC Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L
Description: This alarm indicates that the AC input voltage to the rectifiers is too high or too low.		
Remedial action: Verify and correct the AC power supply to the rectifiers.		

Table 29-341 IK4005041

Alarm	Attributes	Applicable major release
Name: IK4005041 (2339) Type: equipmentAlarm Package: lte.IK4005041 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU AC BATTERY CHARGING FAILURE Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB is operating on the battery power.		
Remedial action: Verify and correct the AC power supply to the rectifiers. If the alarm persists, check and replace any failed rectifier components.		

Table 29-342 IK4005042

Alarm	Attributes	Applicable major release
Name: IK4005042 (2340) Type: equipmentAlarm Package: lte.IK4005042 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU FAN ALARM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the baseband cabinet fan failure.		
Remedial action: Replace the baseband cabinet fan.		

Table 29-343 IK4005043

Alarm	Attributes	Applicable major release
Name: IK4005043 (2341) Type: environmentalAlarm Package: lte.IK4005043 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU DOOR ALARM Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.L
Description: This alarm indicates that the eNodeB door is open.		
Remedial action: Close the cabinet door.		

Table 29-344 IK4005044

Alarm	Attributes	Applicable major release
Name: IK4005044 (2342) Type: environmentalAlarm Package: lte.IK4005044 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU OVER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L

Table 29-344 IK4005044 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the baseband cabinet temperature is above the safe operating threshold.		
Remedial action: Check the cabinet for proper functioning fans and unclogged air filters. Check if the ambient temperature is within the recommended operating range.		

Table 29-345 IK4005045

Alarm	Attributes	Applicable major release
Name: IK4005045 (2343) Type: environmentalAlarm Package: lte.IK4005045 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU UNDER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the baseband cabinet temperature is below the safe operating threshold.		
Remedial action: Check if the ambient temperature is within the recommended operating range.		

Table 29-346 IK4005046

Alarm	Attributes	Applicable major release
Name: IK4005046 (2344) Type: equipmentAlarm Package: lte.IK4005046 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAF Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the baseband cabinet filter airflow is reduced by excessive dirt.		
Remedial action: Replace the fresh air filter.		

Table 29-347 IK4005047

Alarm	Attributes	Applicable major release
Name: IK4005047 (2345) Type: communicationsAlarm Package: lte.IK4005047 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU AUX EQUIP Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an error in the auxiliary telecom equipment in the eNodeB.		
Remedial action: Check the auxiliary telecom equipment.		

Table 29-348 IK4005051

Alarm	Attributes	Applicable major release
Name: IK4005051 (2349) Type: equipmentAlarm Package: lte.IK4005051 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: DBU BACKPLANE TYPE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the backplane type is not supported.		
Remedial action: Proceed with a software upgrade.		

Table 29-349 IK4005052

Alarm	Attributes	Applicable major release
Name: IK4005052 (2350) Type: equipmentAlarm Package: lte.IK4005052 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU RUC FAN FAULT MAJOR Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm Indicates that the fan assemblies cooling capacity has been degraded. RUC I2C communication or cables may be at fault.		
Remedial action: Perform a RUC reset. Power cycle the eNodeB if there is a I2C communication issue. Check the fan hardware assembly and communication cables and connections.		

Table 29-350 IK4005053

Alarm	Attributes	Applicable major release
Name: IK4005053 (2351) Type: equipmentAlarm Package: lte.IK4005053 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: DBU RUC FAN FAULT CRITICAL Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the fan assemblies is not functioning. The RUC I2C communication or cables may be at fault.		
Remedial action: HW autonomously powers down the system.\nCheck the connector between RUC and backplane, it can be damage if the light goes off after removing the front cable so that the backplane does not provides power to the RUC \nCheck the RUC, it can be faulty.		

Table 29-351 IK4005054

Alarm	Attributes	Applicable major release
Name: IK4005054 (2352) Type: equipmentAlarm Package: lte.IK4005054 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU WRONG FAN ASSEMBLY Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a wrong flow RUC, specifically a normal-flow RUC being present when a high-flow RUC is needed.		
Remedial action: Call the next level of support.		

Table 29-352 IK4005055

Alarm	Attributes	Applicable major release
Name: IK4005055 (2999) Type: equipmentAlarm Package: lte.IK4005055 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU HEAT EXCHANGER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the cabinet heat exchanger has failed		
Remedial action: Replace the heat exchanger.		

Table 29-353 IK4005058

Alarm	Attributes	Applicable major release
Name: IK4005058 (3002) Type: equipmentAlarm Package: lte.IK4005058 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-354 IK4005059

Alarm	Attributes	Applicable major release
Name: IK4005059 (3003) Type: equipmentAlarm Package: lte.IK4005059 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		

Table 29-354 IK4005059 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the additional information for maintenance action details.		

Table 29-355 IK4005060

Alarm	Attributes	Applicable major release
Name: IK4005060 (3004) Type: equipmentAlarm Package: lte.IK4005060 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-356 IK4005070

Alarm	Attributes	Applicable major release
Name: IK4005070 (3759) Type: equipmentAlarm Package: lte.IK4005070 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: TRDU FAN FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the TRDU fan has failed.		
Remedial action: Replace the fan.		

Table 29-357 IK4005073

Alarm	Attributes	Applicable major release
Name: IK4005073 (3762) Type: equipmentAlarm Package: lte.IK4005073 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: SMOKE DETECTOR Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • LR15.1.L
Description: This alarm indicates that the alarm is linked to an optional smoke detector inside cabinet.		
Remedial action: Visit basestation to determine cause. Note: Reset the smoke detector.		

Table 29-358 IK4005074

Alarm	Attributes	Applicable major release
Name: IK4005074 (3763) Type: equipmentAlarm Package: lte.IK4005074 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: WATER DETECTOR Implicitly cleared: true Default probable cause: floodDetected	Release: • LR15.1.L
Description: This alarm indicates that the alarm is linked to a water ingress detector inside cabinet.		
Remedial action: Visit basestation to determine cause. Note: Reset the water detector.		

Table 29-359 IK4005075

Alarm	Attributes	Applicable major release
Name: IK4005075 (3764) Type: equipmentAlarm Package: lte.IK4005075 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: MISSING LINK ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Battery thermal probe disconnection of battery thermal probe failure.		
Remedial action: Visit basestation to determine cause repair as needed. Note: Once the fault is corrected the alarm should clear.		

Table 29-360 IK4005077

Alarm	Attributes	Applicable major release
Name: IK4005077 (3766) Type: equipmentAlarm Package: lte.IK4005077 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: BATTERY NOT DETECTED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the DC breaker protecting the battery has tripped OFF.		
Remedial action: Visit basestation and check input to the battery.		

Table 29-361 IK4005079

Alarm	Attributes	Applicable major release
Name: IK4005079 (3768) Type: equipmentAlarm Package: lte.IK4005079 Raised on class: lte.ENBShelfSpecifics	Severity: warning Specific problem: LOW VOLTAGE DETECTION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Batteries are nearly totally discharged, the power system will soon stop.		
Remedial action: Visit basestation and determine battery failure.		

Table 29-362 IK4005080

Alarm	Attributes	Applicable major release
Name: IK4005080 (3769) Type: equipmentAlarm Package: lte.IK4005080 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: BATTERY MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the batteries have reached the end of life and must be replaced.		
Remedial action: Replace batteries.		

Table 29-363 IK4005081

Alarm	Attributes	Applicable major release
Name: IK4005081 (3986) Type: equipmentAlarm Package: lte.IK4005081 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: RECTIFIER FAILURE MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that more than one rectifier has failed.		
Remedial action: Check rectifier for root cause and either replace rectifier or repair if possible.		

Table 29-364 IK4005082

Alarm	Attributes	Applicable major release
Name: IK4005082 (3987) Type: equipmentAlarm Package: lte.IK4005082 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: AC SURGE PROTECTOR FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the AC lightning protector is failed.		
Remedial action: Check for root cause and either replace surge protector or repair if possible.		

Table 29-365 IK4005083

Alarm	Attributes	Applicable major release
Name: IK4005083 (3988) Type: equipmentAlarm Package: lte.IK4005083 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU UNREADABLE MANUFACTURER DATA ATTACHED HW Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-365 IK4005083 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure to read the manufacturer data of an attached HW (e.g. eAM or FAN)		
Remedial action: Reset the eNodeB. Check the cable between controller and RUC.\nCall next level of support, replace RUC unit		

Table 29-366 IK4005084

Alarm	Attributes	Applicable major release
Name: IK4005084 (4650) Type: equipmentAlarm Package: lte.IK4005084 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-367 IK4005085

Alarm	Attributes	Applicable major release
Name: IK4005085 (4651) Type: equipmentAlarm Package: lte.IK4005085 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-368 IK4005086

Alarm	Attributes	Applicable major release
Name: IK4005086 (4652) Type: equipmentAlarm Package: lte.IK4005086 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: SINGLE RECTIFIER FAILURE Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that one rectifier within the DC rectifier equipment has failed.		
Remedial action: Replace the failed rectifier.		

Table 29-369 IK4005087

Alarm	Attributes	Applicable major release
Name: IK4005087 (8576) Type: equipmentAlarm Package: lte.IK4005087 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-370 IK4005088

Alarm	Attributes	Applicable major release
Name: IK4005088 (8577) Type: equipmentAlarm Package: lte.IK4005088 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-371 IK4005089

Alarm	Attributes	Applicable major release
Name: IK4005089 (8578) Type: equipmentAlarm Package: lte.IK4005089 Raised on class: lte.ENBShelfSpecifics	Severity: major Specific problem: DBU FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-372 IK4005090

Alarm	Attributes	Applicable major release
Name: IK4005090 (8579) Type: equipmentAlarm Package: lte.IK4005090 Raised on classes: • lte.ENBShelfSpecifics • lte.MODULE • lte.TmaAldEntry	Severity: critical Specific problem: INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to initialize the associated resources.		
Remedial action: Reset CB using the remote connection to NEM. Check BIST result. If the alarm persists, replace the CB.		

Table 29-373 IK4005091

Alarm	Attributes	Applicable major release
Name: IK4005091 (8580) Type: equipmentAlarm Package: lte.IK4005091 Raised on classes: • lte.ENBShelfSpecifics • lte.MODULE	Severity: major Specific problem: AC MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of multiple rectifier components.		
Remedial action: Replace the failed rectifier component.		

Table 29-374 IK4005092

Alarm	Attributes	Applicable major release
Name: IK4005092 (8581) Type: equipmentAlarm Package: lte.IK4005092 Raised on classes: • lte.ENBShelfSpecifics • lte.MODULE	Severity: minor Specific problem: AC MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a minor failure in the DC rectifier unit.		
Remedial action: Replace the failed fan or the rectifier component.		

Table 29-375 IK4005093

Alarm	Attributes	Applicable major release
Name: IK4005093 (8582) Type: equipmentAlarm Package: lte.IK4005093 Raised on classes: • lte.ENBShelfSpecifics • lte.MODULE	Severity: major Specific problem: AC INPUT OUT OF SPEC Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the AC input voltage to the rectifiers is too high or too low.		
Remedial action: Verify and correct the AC power supply to the rectifiers.		

Table 29-376 IK4005094

Alarm	Attributes	Applicable major release
Name: IK4005094 (8583) Type: equipmentAlarm Package: lte.IK4005094 Raised on classes: • lte.ENBShelfSpecifics • lte.AMR	Severity: major Specific problem: FAN ALARM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the baseband cabinet fan failure.		
Remedial action: Replace the baseband cabinet fan.		

Table 29-377 IK4005095

Alarm	Attributes	Applicable major release
Name: IK4005095 (8584) Type: environmentalAlarm Package: lte.IK4005095 Raised on classes: • lte.ENBShelfSpecifics • lte.MODULE • lte.AMR	Severity: minor Specific problem: DOOR ALARM Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB door is open.		
Remedial action: Close the cabinet door.		

Table 29-378 IK4005096

Alarm	Attributes	Applicable major release
Name: IK4005096 (8585) Type: environmentalAlarm Package: lte.IK4005096 Raised on classes: • lte.ENBShelfSpecifics • lte.AMR	Severity: major Specific problem: OVER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the baseband or RF cabinet temperature is above the safe operating threshold.		
Remedial action: Check for additional cabinet fan or air filter alarms. Check the cabinet for proper functioning fans. Check for clogged air filters. Check if the ambient temperature is within the recommended operating range.		

Table 29-379 IK4005097

Alarm	Attributes	Applicable major release
Name: IK4005097 (8586) Type: equipmentAlarm Package: lte.IK4005097 Raised on classes: • lte.ENBShelfSpecifics • lte.AMR	Severity: minor Specific problem: FAF Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the baseband cabinet filter airflow is reduced by excessive dirt.		
Remedial action: Replace the fresh air filter.		

Table 29-380 IK4005098

Alarm	Attributes	Applicable major release
Name: IK4005098 (8587) Type: equipmentAlarm Package: lte.IK4005098 Raised on classes: • lte.RFM • lte.ENBShelfSpecifics	Severity: major Specific problem: UNREADABLE MANUFACTURER DATA ATTACHED HW Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to read the manufacturer data of an attached HW (e.g. eAM or FAN)		
Remedial action: Reset the CB. Check the cable between controller and RUC.\nCall next level of support, replace RUC unit		

Table 29-381 IK4005101

Alarm	Attributes	Applicable major release
Name: IK4005101 (10053) Type: equipmentAlarm Package: lte.IK4005101 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EVENT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU event detected		
Remedial action: No action is required.		

Table 29-382 IK4005102

Alarm	Attributes	Applicable major release
Name: IK4005102 (10054) Type: equipmentAlarm Package: lte.IK4005102 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EVENT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified DBU event detected		
Remedial action: No action is required.		

Table 29-383 IK4006001

Alarm	Attributes	Applicable major release
Name: IK4006001 (2353) Type: equipmentAlarm Package: lte.IK4006001 Raised on class: lte.RFM	Severity: critical Specific problem: RFM SELF TEST CRITICAL FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the power-on self test detected a critical failure on the RFM. The alarm is cleared when the RFM is reset.		
Remedial action: Reset the RFM. If the alarm persists, replace RFM.		

Table 29-384 IK4006002

Alarm	Attributes	Applicable major release
Name: IK4006002 (2354) Type: equipmentAlarm Package: lte.IK4006002 Raised on class: lte.RFM	Severity: major Specific problem: RFM TXPORT1 OVERCURRENT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the DC-Bias Current for AISG Devices was exceeded on Tx Port 1		

Table 29-384 IK4006002 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check For AISG device in critical alarm or failure mode.		

Table 29-385 IK4006003

Alarm	Attributes	Applicable major release
Name: IK4006003 (2355) Type: processingErrorAlarm Package: lte.IK4006003 Raised on class: lte.RFM	Severity: critical Specific problem: RFM OPERATION PROCESSING FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the fault in the RFM software processing.		
Remedial action: Reset the RFM. If the problem persists, contact the next level support.		

Table 29-386 IK4006004

Alarm	Attributes	Applicable major release
Name: IK4006004 (2356) Type: equipmentAlarm Package: lte.IK4006004 Raised on class: lte.RFM	Severity: warning Specific problem: RFM SFP INCOMPATIBILITY CPRIPORT 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP on the RFM doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the RFM.		

Table 29-387 IK4006005

Alarm	Attributes	Applicable major release
Name: IK4006005 (2357) Type: equipmentAlarm Package: lte.IK4006005 Raised on class: lte.RFM	Severity: warning Specific problem: RFM SFP INCOMPATIBILITY CPRIPORT 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP on the RFM doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the RFM.		

Table 29-388 IK4006006

Alarm	Attributes	Applicable major release
Name: IK4006006 (2358) Type: communicationsAlarm Package: lte.IK4006006 Raised on class: lte.RFM	Severity: critical Specific problem: RFM COMM FAIL Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L
Description: This alarm indicates that no management messages are received in the past 30 seconds, or no active C and M TCP connection.		
Remedial action: Check the RFM, Fiber, and SFPs. Reset the eNodeB.		

Table 29-389 IK4006007

Alarm	Attributes	Applicable major release
Name: IK4006007 (2359) Type: environmentalAlarm Package: lte.IK4006007 Raised on class: lte.RFM	Severity: minor Specific problem: RFM UNDER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFM is below the operating temperature, but is capable of transmitting.		
Remedial action: No action is required.		

Table 29-390 IK4006008

Alarm	Attributes	Applicable major release
Name: IK4006008 (2360) Type: environmentalAlarm Package: lte.IK4006008 Raised on class: lte.RFM	Severity: critical Specific problem: RFM WARM UP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFM temperature is too low to generate RF.		
Remedial action: Check the RFM environment temperature. If RFM has just initialized then wait for it to warm up.		

Table 29-391 IK4006009

Alarm	Attributes	Applicable major release
Name: IK4006009 (2361) Type: environmentalAlarm Package: lte.IK4006009 Raised on class: lte.RFM	Severity: minor Specific problem: RFM OVER TEMP WARNING Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L

Table 29-391 IK4006009 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the RFM is rising near the shutdown limit.		
Remedial action: Check the RFM environment temperature.		

Table 29-392 IK4006010

Alarm	Attributes	Applicable major release
Name: IK4006010 (2362) Type: environmentalAlarm Package: lte.IK4006010 Raised on class: lte.RFM	Severity: critical Specific problem: RFM CRITICAL TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFM temperature is above the operating limit and the transmitter has shut down in an attempt to reduce the temperature.		
Remedial action: Check the RFM environment temperature.		

Table 29-393 IK4006012

Alarm	Attributes	Applicable major release
Name: IK4006012 (2364) Type: equipmentAlarm Package: lte.IK4006012 Raised on class: lte.RFM	Severity: critical Specific problem: RFM INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the FGPA download failure or unlocked PLLs. The evaluation occurs during initialization and the unit is not enabled.		
Remedial action: Reset the RFM. If the alarm persists, replace RFM.		

Table 29-394 IK4006013

Alarm	Attributes	Applicable major release
Name: IK4006013 (2365) Type: processingErrorAlarm Package: lte.IK4006013 Raised on class: lte.RFM	Severity: critical Specific problem: RFM SOFTWARE FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates the general software failures, including TCP/IP stack errors or TCP Allocate Packet errors. This alarm remains asserted for a minimum of 30 seconds.		
Remedial action: If the alarm does not clear in 30 seconds then reset the RFM. If the alarm persists, notify Nokia support.		

Table 29-395 IK4006014

Alarm	Attributes	Applicable major release
Name: IK4006014 (2366) Type: equipmentAlarm Package: lte.IK4006014 Raised on class: lte.RFM	Severity: major Specific problem: RFM SIGNAL QUALITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RFM output spectrum is degraded, but the RF is still enabled.		
Remedial action: Reset the RFM, if the problem persists then replace the RFM.		

Table 29-396 IK4006016

Alarm	Attributes	Applicable major release
Name: IK4006016 (2368) Type: equipmentAlarm Package: lte.IK4006016 Raised on class: lte.RFM	Severity: warning Specific problem: RFM SFP INCOMPATIBILITY CPRIPORT 3 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the equipped SFP on the RFM doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP on the RFM.		

Table 29-397 IK4006027

Alarm	Attributes	Applicable major release
Name: IK4006027 (2378) Type: equipmentAlarm Package: lte.IK4006027 Raised on class: lte.RFM	Severity: major Specific problem: RFM INPUT VOLTAGE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the input voltage is very high or very low.		
Remedial action: Verify and correct the DC input voltage. If the alarm persists, replace the RFM.		

Table 29-398 IK4006028

Alarm	Attributes	Applicable major release
Name: IK4006028 (2379) Type: equipmentAlarm Package: lte.IK4006028 Raised on class: lte.RFM	Severity: critical Specific problem: RFM PWR CONVERTER FAIL Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L
Description: The RFM internal power converter has failed.		

Table 29-398 IK4006028 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the RFM, if the alarm persists, replace the RFM.		

Table 29-399 IK4006029

Alarm	Attributes	Applicable major release
Name: IK4006029 (2380) Type: equipmentAlarm Package: lte.IK4006029 Raised on class: lte.RFM	Severity: critical Specific problem: RFM CLOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The RFM cannot derive proper clock signal from the incoming CPRI link.		
Remedial action: Verify the CPRI connection and reset the RFM. If the problem persists then replace the RFM.		

Table 29-400 IK4006030

Alarm	Attributes	Applicable major release
Name: IK4006030 (2381) Type: equipmentAlarm Package: lte.IK4006030 Raised on class: lte.RFM	Severity: critical Specific problem: RFM RF SYNTH FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The RFM internal frequency synthesizer is out of lock.		
Remedial action: Reset the RFM. If the problem persists then replace the RFM.		

Table 29-401 IK4006039

Alarm	Attributes	Applicable major release
Name: IK4006039 (2386) Type: equipmentAlarm Package: lte.IK4006039 Raised on class: lte.RFM	Severity: warning Specific problem: RFM UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to read the manufacturer data.		
Remedial action: Reset the RFM. If the alarm persists contact the next level support.		

Table 29-402 IK4006042

Alarm	Attributes	Applicable major release
Name: IK4006042 (2387) Type: processingErrorAlarm Package: lte.IK4006042 Raised on class: lte.RFM	Severity: minor Specific problem: RFM DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates the RFM software download failure.		
Remedial action: Reset the RFM to retry the download. If the problem persists, contact the next level support.		

Table 29-403 IK4006075

Alarm	Attributes	Applicable major release
Name: IK4006075 (2394) Type: equipmentAlarm Package: lte.IK4006075 Raised on class: lte.RFM	Severity: major Specific problem: RFM BIST PARTIAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that at least one failure was detected during power on self-test, but the unit may still be functional, though in a degraded state.		
Remedial action: Replace the RFM.		

Table 29-404 IK4006085

Alarm	Attributes	Applicable major release
Name: IK4006085 (2404) Type: equipmentAlarm Package: lte.IK4006085 Raised on class: lte.RFM	Severity: minor Specific problem: RFM EXTERNAL UNIT COMM FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the loss of communication with external alarm or filter module.		
Remedial action: Check external module and cable, replace if necessary.		

Table 29-405 IK4006158

Alarm	Attributes	Applicable major release
Name: IK4006158 (2477) Type: equipmentAlarm Package: lte.IK4006158 Raised on class: lte.RFM	Severity: critical Specific problem: RFM ANT CAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the antenna is out of calibration in a cell.		

Table 29-405 IK4006158 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the antenna calibration.		

Table 29-406 IK4006159

Alarm	Attributes	Applicable major release
Name: IK4006159 (2478) Type: equipmentAlarm Package: lte.IK4006159 Raised on class: lte.RFM	Severity: major Specific problem: RFM ANT PERIODIC CAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the antenna periodic calibration has failed.		
Remedial action: Check the antenna calibration.		

Table 29-407 IK4006197

Alarm	Attributes	Applicable major release
Name: IK4006197 (2516) Type: equipmentAlarm Package: lte.IK4006197 Raised on class: lte.RFM	Severity: minor Specific problem: RFM MESSAGE THROTTLING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the RFM is generating too many messages over the CPRI link.		
Remedial action: Reset the RFM.		

Table 29-408 IK4006215

Alarm	Attributes	Applicable major release
Name: IK4006215 (3009) Type: equipmentAlarm Package: lte.IK4006215 Raised on class: lte.RFM	Severity: minor Specific problem: RFM FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-409 IK4006216

Alarm	Attributes	Applicable major release
Name: IK4006216 (3010) Type: equipmentAlarm Package: lte.IK4006216 Raised on class: lte.RFM	Severity: minor Specific problem: RFM FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-410 IK4006217

Alarm	Attributes	Applicable major release
Name: IK4006217 (3011) Type: equipmentAlarm Package: lte.IK4006217 Raised on class: lte.RFM	Severity: minor Specific problem: RFM FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-411 IK4006218

Alarm	Attributes	Applicable major release
Name: IK4006218 (3012) Type: equipmentAlarm Package: lte.IK4006218 Raised on class: lte.RFM	Severity: minor Specific problem: RFM FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-412 IK4006219

Alarm	Attributes	Applicable major release
Name: IK4006219 (3013) Type: equipmentAlarm Package: lte.IK4006219 Raised on class: lte.RFM	Severity: major Specific problem: RFM UNREADABLE MANUFACTURER DATA ATTACHED HW Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-412 IK4006219 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure to read the inventory record of an attached hardware (e.g. RDEM).		
Remedial action: Check the attached hardware.		

Table 29-413 IK4006253

Alarm	Attributes	Applicable major release
Name: IK4006253 (3031) Type: equipmentAlarm Package: lte.IK4006253 Raised on class: lte.RFM	Severity: minor Specific problem: RFM SIGNAL LOW PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-414 IK4006254

Alarm	Attributes	Applicable major release
Name: IK4006254 (3032) Type: equipmentAlarm Package: lte.IK4006254 Raised on class: lte.RFM	Severity: minor Specific problem: RFM SIGNAL LOW PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-415 IK4006255

Alarm	Attributes	Applicable major release
Name: IK4006255 (3033) Type: equipmentAlarm Package: lte.IK4006255 Raised on class: lte.RFM	Severity: minor Specific problem: RFM SIGNAL LOW PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-416 IK4006256

Alarm	Attributes	Applicable major release
Name: IK4006256 (3034) Type: equipmentAlarm Package: lte.IK4006256 Raised on class: lte.RFM	Severity: major Specific problem: RFM TRANS TX FAILURE PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates a failure of the optical transceiver.		
Remedial action: Replace the RFM SFP		

Table 29-417 IK4006257

Alarm	Attributes	Applicable major release
Name: IK4006257 (3035) Type: equipmentAlarm Package: lte.IK4006257 Raised on class: lte.RFM	Severity: major Specific problem: RFM TRANS TX FAILURE PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates a failure of the optical transceiver.		
Remedial action: Replace the RFM SFP		

Table 29-418 IK4006258

Alarm	Attributes	Applicable major release
Name: IK4006258 (3036) Type: equipmentAlarm Package: lte.IK4006258 Raised on class: lte.RFM	Severity: major Specific problem: RFM TRANS TX FAILURE PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates a failure of the optical transceiver.		
Remedial action: Replace the RFM SFP		

Table 29-419 IK4006259

Alarm	Attributes	Applicable major release
Name: IK4006259 (3037) Type: equipmentAlarm Package: lte.IK4006259 Raised on class: lte.RFM	Severity: minor Specific problem: RFM BER PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-420 IK4006260

Alarm	Attributes	Applicable major release
Name: IK4006260 (3038) Type: equipmentAlarm Package: lte.IK4006260 Raised on class: lte.RFM	Severity: minor Specific problem: RFM BER PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-421 IK4006261

Alarm	Attributes	Applicable major release
Name: IK4006261 (3039) Type: equipmentAlarm Package: lte.IK4006261 Raised on class: lte.RFM	Severity: minor Specific problem: RFM BER PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-422 IK4006262

Alarm	Attributes	Applicable major release
Name: IK4006262 (3040) Type: equipmentAlarm Package: lte.IK4006262 Raised on class: lte.RFM	Severity: major Specific problem: RFM SIGNAL SDI PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: Reset RFM. If the alarm persists then reset the eNodeB.		

Table 29-423 IK4006263

Alarm	Attributes	Applicable major release
Name: IK4006263 (3041) Type: equipmentAlarm Package: lte.IK4006263 Raised on class: lte.RFM	Severity: major Specific problem: RFM SIGNAL SDI PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: Reset RFM. If the alarm persists then reset the eNodeB.		

Table 29-424 IK4006264

Alarm	Attributes	Applicable major release
Name: IK4006264 (3042) Type: equipmentAlarm Package: lte.IK4006264 Raised on class: lte.RFM	Severity: major Specific problem: RFM SIGNAL SDI PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: Reset RFM. If the alarm persists then reset the eNodeB.		

Table 29-425 IK4006265

Alarm	Attributes	Applicable major release
Name: IK4006265 (3043) Type: equipmentAlarm Package: lte.IK4006265 Raised on class: lte.RFM	Severity: major Specific problem: RFM DL IDLE PATTERN MISMATCH Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that DL idle patterns are detected (delay calibration failure).		
Remedial action: Reset the RFM. If the alarm persists, call the next level of support.		

Table 29-426 IK4006280

Alarm	Attributes	Applicable major release
Name: IK4006280 (3770) Type: equipmentAlarm Package: lte.IK4006280 Raised on class: lte.RFM	Severity: critical Specific problem: RFM RF PATHS NOT AVAILABLE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM is shared with another technology which has locked the RFM operation.		
Remedial action: Enable the RFM operation through the other technology OMC.		

Table 29-427 IK4006281

Alarm	Attributes	Applicable major release
Name: IK4006281 (3651) Type: communicationsAlarm Package: lte.IK4006281 Raised on class: lte.RFM	Severity: major Specific problem: RFM INTERNAL RRH COMM FAIL Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Communication has failed between the two subunits that make up this RFM.		

Table 29-427 IK4006281 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the inter-subunit CPRI link and SFPs for failure check the far end subunit for failure. Reset the RFM if no physical failure is found.		

Table 29-428 IK4006282

Alarm	Attributes	Applicable major release
Name: IK4006282 (3652) Type: equipmentAlarm Package: lte.IK4006282 Raised on class: lte.RFM	Severity: critical Specific problem: RFM HW CONFIG MISMATCH Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The two subunits that make up this RFM are not of the same type.		
Remedial action: Replace one or both subunits so that they are both of the same type.		

Table 29-429 IK4006283

Alarm	Attributes	Applicable major release
Name: IK4006283 (3653) Type: equipmentAlarm Package: lte.IK4006283 Raised on class: lte.RFM	Severity: critical Specific problem: RFM HW ASSIGNMENT INDETERMINATE Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The two subunits that make up this RFM are both configured with the same subunit number.		
Remedial action: Ensure that each RFM subunit has the proper connector to indicate that it is the first or the second subunit.		

Table 29-430 IK4006284

Alarm	Attributes	Applicable major release
Name: IK4006284 (3654) Type: equipmentAlarm Package: lte.IK4006284 Raised on class: lte.RFM	Severity: minor Specific problem: RFM ALD BUS OVERCURRENT Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The AISG bus attached to this RFM is drawing too much DC electric current.		
Remedial action: Ensure that the number of AISG devices and their individual current loads do not exceed the RFM limit. Check the AISG bus cable for short circuit, check for one or more failed AISG devices on the bus.		

Table 29-431 IK4006285

Alarm	Attributes	Applicable major release
Name: IK4006285 (3655) Type: equipmentAlarm Package: lte.IK4006285 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOF PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that framing cannot be recovered at the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-432 IK4006286

Alarm	Attributes	Applicable major release
Name: IK4006286 (3656) Type: equipmentAlarm Package: lte.IK4006286 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOF PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that framing cannot be recovered at the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-433 IK4006287

Alarm	Attributes	Applicable major release
Name: IK4006287 (3657) Type: equipmentAlarm Package: lte.IK4006287 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOF PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that framing cannot be recovered at the slave link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-434 IK4006288

Alarm	Attributes	Applicable major release
Name: IK4006288 (3658) Type: equipmentAlarm Package: lte.IK4006288 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOS PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-435 IK4006289

Alarm	Attributes	Applicable major release
Name: IK4006289 (3659) Type: equipmentAlarm Package: lte.IK4006289 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOS PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-436 IK4006290

Alarm	Attributes	Applicable major release
Name: IK4006290 (3660) Type: equipmentAlarm Package: lte.IK4006290 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK LOS PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-437 IK4006291

Alarm	Attributes	Applicable major release
Name: IK4006291 (3661) Type: equipmentAlarm Package: lte.IK4006291 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK RAI PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-438 IK4006292

Alarm	Attributes	Applicable major release
Name: IK4006292 (3662) Type: equipmentAlarm Package: lte.IK4006292 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK RAI PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-439 IK4006293

Alarm	Attributes	Applicable major release
Name: IK4006293 (3663) Type: equipmentAlarm Package: lte.IK4006293 Raised on class: lte.RFM	Severity: major Specific problem: RFM LINK RAI PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or CB end).		

Table 29-440 IK4006295

Alarm	Attributes	Applicable major release
Name: IK4006295 (3772) Type: securityServiceOrMechanismViolation Package: lte.IK4006295 Raised on class: lte.RFM	Severity: minor Specific problem: RFM ACCESS PANEL OPEN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the access panel for the RFM maintenance port is open.		
Remedial action: Close the maintenance port access door.		

Table 29-441 IK4006296

Alarm	Attributes	Applicable major release
Name: IK4006296 (3773) Type: equipmentAlarm Package: lte.IK4006296 Raised on class: lte.RFM	Severity: major Specific problem: RFM CELL DATA CONFLICT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM is shared by two technologies and one technology controller has attempted to configure a cell on the RFM which conflicts in frequency or transmit power setting with an existing configured cell.		
Remedial action: Change the cell settings (eARFCN assignment, downlink power setting) for the RFM so that they are compatible (cell frequencies do not overlap, cell frequency settings do not exceed the RFM bandwidth, etc.). Since this is a shared RFM, the cell settings may reside in different databases.		

Table 29-442 IK4006297

Alarm	Attributes	Applicable major release
Name: IK4006297 (3774) Type: equipmentAlarm Package: lte.IK4006297 Raised on class: lte.RFM	Severity: critical Specific problem: RF SETUP FAULT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM is currently transmitting and has received a new carrier configuration request that requires a disruption to transmission.		
Remedial action: Lock the carriers (both technologies if this is a shared RFM) to disable transmission, the RFM will retune and clear the alarm. Carriers may then be unlocked.		

Table 29-443 IK4006298

Alarm	Attributes	Applicable major release
Name: IK4006298 (3775) Type: equipmentAlarm Package: lte.IK4006298 Raised on class: lte.RFM	Severity: major Specific problem: RFM DATA SYNCHRONIZATION FAULT Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM is shared by two technologies and one technology is transmitting CPRI data at a different rate than the other.		
Remedial action: Check the timing reference sources for both baseband units for failures.		

Table 29-444 IK4006301

Alarm	Attributes	Applicable major release
Name: IK4006301 (3777) Type: equipmentAlarm Package: lte.IK4006301 Raised on class: lte.RFM	Severity: major Specific problem: RFM TXPORT2 OVERCURRENT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the DC-Bias Current for AISG Devices was exceeded on Tx Port 2		
Remedial action: Check For AISG device in critical alarm or failure mode.		

Table 29-445 IK4006302

Alarm	Attributes	Applicable major release
Name: IK4006302 (3778) Type: equipmentAlarm Package: lte.IK4006302 Raised on class: lte.RFM	Severity: major Specific problem: RFM AISG PORT OVERCURRENT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the DC-Bias Current for AISG Devices was exceeded on RS-485 Port		
Remedial action: Check For AISG device in critical alarm or failure mode.		

Table 29-446 IK4006303

Alarm	Attributes	Applicable major release
Name: IK4006303 (3779) Type: equipmentAlarm Package: lte.IK4006303 Raised on class: lte.RFM	Severity: major Specific problem: RFM DC-BIAS OVERCURRENT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the DC-Bias Current Source in the RFM exceeded the maximum threshold.		
Remedial action: Check that the number of ALDs device supported by the RFM are within the maximum number and/or none of them is in failure mode.		

Table 29-447 IK4006304

Alarm	Attributes	Applicable major release
Name: IK4006304 (4653) Type: equipmentAlarm Package: lte.IK4006304 Raised on class: lte.RFM	Severity: critical Specific problem: RRH DC POWER OFF Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM DC power supply is off.		
Remedial action: Check the DC power supply for failure, both internal and external to the RFM.		

Table 29-448 IK4006307

Alarm	Attributes	Applicable major release
Name: IK4006307 (4654) Type: environmentalAlarm Package: lte.IK4006307 Raised on class: lte.RFM	Severity: major Specific problem: RFM FAN1 FAILED Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-448 IK4006307 (continued)

Alarm	Attributes	Applicable major release
Description: Fan 1 in the RFM has failed.		
Remedial action: Replace the failed hardware.		

Table 29-449 IK4006308

Alarm	Attributes	Applicable major release
Name: IK4006308 (4655) Type: environmentalAlarm Package: lte.IK4006308 Raised on class: lte.RFM	Severity: major Specific problem: RFM FAN2 FAILED Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Fan 2 in the RFM has failed.		
Remedial action: Replace the failed hardware.		

Table 29-450 IK4006309

Alarm	Attributes	Applicable major release
Name: IK4006309 (4656) Type: environmentalAlarm Package: lte.IK4006309 Raised on class: lte.RFM	Severity: critical Specific problem: RFM BOTH FANS FAILED Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L
Description: Both fans in the RFM have failed.		
Remedial action: Replace the failed hardware.		

Table 29-451 IK4006310

Alarm	Attributes	Applicable major release
Name: IK4006310 (8588) Type: equipmentAlarm Package: lte.IK4006310 Raised on class: lte.RFM	Severity: minor Specific problem: RFM FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-452 IK4006311

Alarm	Attributes	Applicable major release
Name: IK4006311 (8589) Type: equipmentAlarm Package: lte.IK4006311 Raised on class: lte.RFM	Severity: major Specific problem: RFM FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFM fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-453 IK4006312

Alarm	Attributes	Applicable major release
Name: IK4006312 (8590) Type: equipmentAlarm Package: lte.IK4006312 Raised on class: lte.RFM	Severity: minor Specific problem: SFP FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-454 IK4006321

Alarm	Attributes	Applicable major release
Name: IK4006321 (8591) Type: communicationsAlarm Package: lte.IK4006321 Raised on classes: • lte.RFM • lte.RFME • lte.AMR	Severity: critical Specific problem: COMM FAIL Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that no management messages are received in the past 30 seconds, or no active C and M TCP connection.		
Remedial action: Check the RFM, Fiber, and SFPs. Reset the CB.		

Table 29-455 IK4006322

Alarm	Attributes	Applicable major release
Name: IK4006322 (8592) Type: environmentalAlarm Package: lte.IK4006322 Raised on classes: • lte.RFM • lte.ENBShelfSpecifics • lte.RFME	Severity: minor Specific problem: UNDER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the unit's temperature is below the operating limits, but is still capable of providing service.		
Remedial action: No action is required.		

Table 29-456 IK4006324

Alarm	Attributes	Applicable major release
Name: IK4006324 (8593) Type: environmentalAlarm Package: lte.IK4006324 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: CRITICAL TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM temperature is above the operating limit and the transmitter has shut down in an attempt to reduce the temperature.		
Remedial action: Check the RFM environment temperature.		

Table 29-457 IK4006325

Alarm	Attributes	Applicable major release
Name: IK4006325 (8594) Type: equipmentAlarm Package: lte.IK4006325 Raised on classes: • lte.RFM • lte.RFME	Severity: major Specific problem: SIGNAL QUALITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM output spectrum is degraded, but the RF is still enabled.		
Remedial action: Reset the RFM, if the problem persists then replace the RFM.		

Table 29-458 IK4006326

Alarm	Attributes	Applicable major release
Name: IK4006326 (8595) Type: equipmentAlarm Package: lte.IK4006326 Raised on classes: • lte.RFM • lte.RFME	Severity: major Specific problem: INPUT VOLTAGE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the input voltage is very high or very low.		
Remedial action: Verify and correct the DC input voltage. If the alarm persists, replace the RFM.		

Table 29-459 IK4006327

Alarm	Attributes	Applicable major release
Name: IK4006327 (8596) Type: equipmentAlarm Package: lte.IK4006327 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: PWR CONVERTER FAIL Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM internal power converter has failed.		
Remedial action: Reset the RFM, if the alarm persists, replace the RFM.		

Table 29-460 IK4006328

Alarm	Attributes	Applicable major release
Name: IK4006328 (8597) Type: equipmentAlarm Package: lte.IK4006328 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: CLOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM cannot derive proper clock signal from the incoming CPRI link.		
Remedial action: Verify the CPRI connection and reset the RFM. If the problem persists then replace the RFM.		

Table 29-461 IK4006329

Alarm	Attributes	Applicable major release
Name: IK4006329 (8598) Type: equipmentAlarm Package: lte.IK4006329 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: RF SYNTH FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM internal frequency synthesizer is out of lock.		
Remedial action: Reset the RFM. If the problem persists then replace the RFM.		

Table 29-462 IK4006331

Alarm	Attributes	Applicable major release
Name: IK4006331 (8599) Type: equipmentAlarm Package: lte.IK4006331 Raised on classes: • lte.RFM • lte.RFME	Severity: major Specific problem: BIST PARTIAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that at least one failure was detected during power on self-test, but the unit may still be functional, though in a degraded state.		
Remedial action: Replace the RFM.		

Table 29-463 IK4006332

Alarm	Attributes	Applicable major release
Name: IK4006332 (8600) Type: equipmentAlarm Package: lte.IK4006332 Raised on classes: • lte.RFM • lte.RFME	Severity: minor Specific problem: MESSAGE THROTTLING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM is generating too many messages over the CPRI link.		
Remedial action: Reset the RFM.		

Table 29-464 IK4006333

Alarm	Attributes	Applicable major release
Name: IK4006333 (8601) Type: environmentalAlarm Package: lte.IK4006333 Raised on classes: • lte.RFM • lte.RFME	Severity: minor Specific problem: OVER TEMP WARNING Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM is rising near the shutdown limit.		
Remedial action: Check the RFM environment temperature.		

Table 29-465 IK4006334

Alarm	Attributes	Applicable major release
Name: IK4006334 (8602) Type: equipmentAlarm Package: lte.IK4006334 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-466 IK4006335

Alarm	Attributes	Applicable major release
Name: IK4006335 (8603) Type: equipmentAlarm Package: lte.IK4006335 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-467 IK4006336

Alarm	Attributes	Applicable major release
Name: IK4006336 (8604) Type: equipmentAlarm Package: lte.IK4006336 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-468 IK4006337

Alarm	Attributes	Applicable major release
Name: IK4006337 (8605) Type: equipmentAlarm Package: lte.IK4006337 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-469 IK4006338

Alarm	Attributes	Applicable major release
Name: IK4006338 (8606) Type: equipmentAlarm Package: lte.IK4006338 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-470 IK4006339

Alarm	Attributes	Applicable major release
Name: IK4006339 (8607) Type: equipmentAlarm Package: lte.IK4006339 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-470 IK4006339 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-471 IK4006340

Alarm	Attributes	Applicable major release
Name: IK4006340 (8608) Type: equipmentAlarm Package: lte.IK4006340 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-472 IK4006341

Alarm	Attributes	Applicable major release
Name: IK4006341 (8609) Type: equipmentAlarm Package: lte.IK4006341 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-473 IK4006342

Alarm	Attributes	Applicable major release
Name: IK4006342 (8610) Type: equipmentAlarm Package: lte.IK4006342 Raised on class: lte.RFM	Severity: major Specific problem: RFM PORT1 SYNCHRONIZATION FAULT Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates the RFM is shared by two technologies and one technology is transmitting CPRI data at a different rate than the other.		
Remedial action: Check the timing reference sources for both baseband units for failures.		

Table 29-474 IK4006343

Alarm	Attributes	Applicable major release
Name: IK4006343 (8611) Type: equipmentAlarm Package: lte.IK4006343 Raised on class: lte.RFM	Severity: major Specific problem: RFM PORT2 SYNCHRONIZATION FAULT Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates the RFM is shared by two technologies and one technology is transmitting CPRI data at a different rate than the other.		
Remedial action: Check the timing reference sources for both baseband units for failures.		

Table 29-475 IK4006344

Alarm	Attributes	Applicable major release
Name: IK4006344 (8612) Type: equipmentAlarm Package: lte.IK4006344 Raised on class: lte.RFM	Severity: major Specific problem: RFM PORT3 SYNCHRONIZATION FAULT Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates the RFM is shared by two technologies and one technology is transmitting CPRI data at a different rate than the other.		
Remedial action: Check the timing reference sources for both baseband units for failures.		

Table 29-476 IK4006345

Alarm	Attributes	Applicable major release
Name: IK4006345 (8613) Type: equipmentAlarm Package: lte.IK4006345 Raised on class: lte.RFM	Severity: critical Specific problem: RFM CRITICAL FAULT IN SECONDARY MODE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM has a critical fault. The RFM is in shared mode and LTE is the secondary user. Fault management of the shared RFM is performed by the primary operator/technology (GSM/WCDMA/CDMA), which has detailed information about the fault.		
Remedial action: Contact the primary operator/technology of the RFM and request to fix the issue. Then LOCK/UNLOCK the unit.		

Table 29-477 IK4006354

Alarm	Attributes	Applicable major release
Name: IK4006354 (10055) Type: environmentalAlarm Package: lte.IK4006354 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: WARM UP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCool-ingSystemProblem	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM temperature is too low to generate RF.		
Remedial action: Check the RFM environment temperature. If RFM has just initialized then wait for it to warm up.		

Table 29-478 IK4006355

Alarm	Attributes	Applicable major release
Name: IK4006355 (10056) Type: equipmentAlarm Package: lte.IK4006355 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: SELF TEST CRITICAL FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the power-on self test detected a critical failure on the RFM. The alarm is cleared when the RFM is reset.		
Remedial action: Reset the RFM. If the alarm persists, replace RFM.		

Table 29-479 IK4007001

Alarm	Attributes	Applicable major release
Name: IK4007001 (2533) Type: processingErrorAlarm Package: lte.IK4007001 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BRC CC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BRC-CC reported a warning.		
Remedial action: No action is required.		

Table 29-480 IK4007002

Alarm	Attributes	Applicable major release
Name: IK4007002 (2534) Type: processingErrorAlarm Package: lte.IK4007002 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BRC UC FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the UeCallIP detected a no-response from BRC-UC.		
Remedial action: No action is required.		

Table 29-481 IK4007003

Alarm	Attributes	Applicable major release
Name: IK4007003 (5214) Type: operationalViolation Package: lte.IK4007003 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: PCI POTENTIAL CONFUSION VICTIM Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates this eNB is potentially a victim of PCI confusion, it has multiple potential neighbor cells that have the same PCI as each other.		
Remedial action: The maintenance action has to be done in one of the neighbor eNBs.\nNote that here only a potential confusion is raised, meaning that there may be no impact.\nIn case HO KPIs show an issue, this may be the cause.\nThen a manual intervention, is needed in one of the distant eNBs to solve the problem, by changing the PCI.\nIf the Neighbours are confirmed to be real, then the confusion is detected as real and AutoPCI will try to solve the conflict on the actor side. In case it is not enabled or it cannot solve the conflict, major alarms are raised on both actor and victim sides.		

Table 29-482 IK4007004

Alarm	Attributes	Applicable major release
Name: IK4007004 (2535) Type: processingErrorAlarm Package: lte.IK4007004 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BRC UC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BRC-UC reported a warning.		
Remedial action: No action is required.		

Table 29-483 IK4007005

Alarm	Attributes	Applicable major release
Name: IK4007005 (2536) Type: processingErrorAlarm Package: lte.IK4007005 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLP MANAGER WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that CallP Manager reports a warning.		
Remedial action: No action is required.		

Table 29-484 IK4007006

Alarm	Attributes	Applicable major release
Name: IK4007006 (2537) Type: processingErrorAlarm Package: lte.IK4007006 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CELL CALLP WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that Cell CallP reports a warning.		
Remedial action: No action is required.		

Table 29-485 IK4007007

Alarm	Attributes	Applicable major release
Name: IK4007007 (5215) Type: processingErrorAlarm Package: lte.IK4007007 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: RFTRACE ACTIVATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to activate a new RF trace recording session.		
Remedial action: No action is required.		

Table 29-486 IK4007009

Alarm	Attributes	Applicable major release
Name: IK4007009 (5216) Type: qualityOfServiceAlarm Package: lte.IK4007009 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE SESSION PREEMPTION INDICATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-486 IK4007009 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that one or several sessions have been pre-empted (suspended for the considered MbsfnArea) in order to admit a higher priority session.		
Remedial action: No action is required.		

Table 29-487 IK4007010

Alarm	Attributes	Applicable major release
Name: IK4007010 (2539) Type: qualityOfServiceAlarm Package: lte.IK4007010 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE SESSION RESUME INDICATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that one or several sessions previously pre-empted have been resumed (resumed for the considered MbsfnArea).		
Remedial action: No action is required.		

Table 29-488 IK4007011

Alarm	Attributes	Applicable major release
Name: IK4007011 (2540) Type: operationalViolation Package: lte.IK4007011 Raised on class: lte.Cell	Severity: major Specific problem: PCI CONFUSION VICTIM Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates this cell is victim of PCI confusion, it has multiple real neighbor cells that have the same PCI as each other.\nA manual intervention is needed to solve the problem.		
Remedial action: The maintenance action has to be done in one of the neighbor eNBs.\nIf AutoPCI is not activated in these eNBs, then the manual intervention consists in changing the PCI.\nIf AutoPCI is activated in these eNBs, then the manual intervention consists in changing some constraints (e.g. increase the pciAllowedList)		

Table 29-489 IK4007012

Alarm	Attributes	Applicable major release
Name: IK4007012 (2541) Type: qualityOfServiceAlarm Package: lte.IK4007012 Raised on class: lte.Cell	Severity: indeterminate Specific problem: VERY HIGH RACH ARRIVAL RATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNB has triggered Access Class Barring in a cell due to RACH overload.		

Table 29-489 IK4007012 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-490 IK4007013

Alarm	Attributes	Applicable major release
Name: IK4007013 (2542) Type: processingErrorAlarm Package: lte.IK4007013 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: RFTRACE INVALID PARAMETER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the parameter received for RF trace is invalid.		
Remedial action: No action is required.		

Table 29-491 IK4007015

Alarm	Attributes	Applicable major release
Name: IK4007015 (5218) Type: qualityOfServiceAlarm Package: lte.IK4007015 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CAC FAILURE BEGIN Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallP reported a CAC failure.		
Remedial action: No action is required.		

Table 29-492 IK4007016

Alarm	Attributes	Applicable major release
Name: IK4007016 (5219) Type: qualityOfServiceAlarm Package: lte.IK4007016 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CAC FAILURE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallP reported the expiration of the monitoring time interval timer.		
Remedial action: No action is required.		

Table 29-493 IK4007017

Alarm	Attributes	Applicable major release
Name: IK4007017 (5220) Type: communicationsAlarm Package: lte.IK4007017 Raised on class: lte.Cell	Severity: critical Specific problem: CONFIRMED COMMUNICATION ISSUE MET WITH UE SETUPS ON THIS CELL Implicitly cleared: true Default probable cause: applicationSubsystemFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that an internal communication issue has been met for multiple UEs on this cell during the UE Setup procedure.		
Remedial action: Lock and then unlock the LteCell. If this fails to clear the fault then lock and unlock the modem (BB) board.		

Table 29-494 IK4007018

Alarm	Attributes	Applicable major release
Name: IK4007018 (5221) Type: operationalViolation Package: lte.IK4007018 Raised on class: lte.ENBEquipment	Severity: major Specific problem: PCI CONFUSION NEIGHB CELLS Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates this eNB is a victim of PCI confusion, it has multiple neighbor cells that have the same PCI as each other.\nA manual intervention is needed to solve the problem. This issue may affect mobility procedures in any of the eNodeB cells.		
Remedial action: The maintenance action has to be done in one of the neighbour eNBs.The issue is also reported by Alarms in these eNBs. If the automatic PCI allocation is activated in these eNBs:(1) If a Warning Alarm is raised, the issue will be automatically solved in the next maintenance window; (2) If a Major Alarm is raised, the issue cannot be automatically solved. It is necessary to increase the list of allowed PCI values, and the issue will be automatically solved in the next maintenance window. If the automatic PCI allocation is not activated in these eNBs:A Major Alarm is raised. It is necessary to change the PCI value of one of the actor cell of the issue.		

Table 29-495 IK4007019

Alarm	Attributes	Applicable major release
Name: IK4007019 (2543) Type: processingErrorAlarm Package: lte.IK4007019 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: UBM FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a non-response of UBM entity detected by UeCallP.		
Remedial action: No action is required.		

Table 29-496 IK4007020

Alarm	Attributes	Applicable major release
Name: IK4007020 (5222) Type: operationalViolation Package: lte.IK4007020 Raised on class: lte.Cell	Severity: major Specific problem: PCI CONFUSION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI confusion between the cell and a neighbour cell of a neighbour cell. A manual intervention is needed to solve the problem. This can happen in the following cases: (1)The conflict could not be solved autonomously by the eNB; (2)The automatic PCI allocation is not activated.		
Remedial action: If the automatic PCI allocation is activated: Increase the list of allowed PCI values, either for the local or for the distant eNodeB; If the automatic PCI allocation is not activated:Change the PCI value, either for the local or the distant cell.		

Table 29-497 IK4007021

Alarm	Attributes	Applicable major release
Name: IK4007021 (2544) Type: processingErrorAlarm Package: lte.IK4007021 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: UE CALLP WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a warning reported by UeCallP.		
Remedial action: No action is required.		

Table 29-498 IK4007022

Alarm	Attributes	Applicable major release
Name: IK4007022 (2545) Type: communicationsAlarm Package: lte.IK4007022 Raised on class: lte.MmeAccess	Severity: critical Specific problem: MME S1 SETUP FAILURE RESPONSE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent S1_SETUP_FAILURE_RESPONSE from MME detected by CallIPMgr.		
Remedial action: Check the behavior of the MME.		

Table 29-499 IK4007023

Alarm	Attributes	Applicable major release
Name: IK4007023 (2546) Type: communicationsAlarm Package: lte.IK4007023 Raised on class: lte.MmeAccess	Severity: critical Specific problem: MME S1 SETUP NO RESPONSE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent NO_RESPONSE from MME detected by CallIPMgr.		
Remedial action: Check the behavior of the MME.		

Table 29-500 IK4007024

Alarm	Attributes	Applicable major release
Name: IK4007024 (5223) Type: integrityViolation Package: lte.IK4007024 Raised on class: lte.Mce	Severity: indeterminate Specific problem: TIME FOR SESSION START STOP or UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that there is no absolute time has been provided in any received M3 MBMS Session Start Request, M3 MBMS Session Stop Request or M3 MBMS Session Update Request message.		
Remedial action: No action is required.		

Table 29-501 IK4007025

Alarm	Attributes	Applicable major release
Name: IK4007025 (5224) Type: qualityOfServiceAlarm Package: lte.IK4007025 Raised on class: lte.Cell	Severity: indeterminate Specific problem: IMMEDIATE LOAD CONTROL BEGIN Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicate that immediate load control procedure begins.		
Remedial action: No action is required.		

Table 29-502 IK4007026

Alarm	Attributes	Applicable major release
Name: IK4007026 (2547) Type: communicationsAlarm Package: lte.IK4007026 Raised on class: lte.X2Access	Severity: critical Specific problem: ENB CANDIDATE X2 SETUP FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent X2_SETUP_FAILURE from eNodeB_CANDIDATE detected by CallpMgr.		
Remedial action: Check the behavior of the candidate eNodeB. If the alarm persists, check provisioning of the initiating and candidate eNodeBs.		

Table 29-503 IK4007027

Alarm	Attributes	Applicable major release
Name: IK4007027 (2548) Type: communicationsAlarm Package: lte.IK4007027 Raised on class: lte.X2Access	Severity: critical Specific problem: ENB CANDIDATE X2 SETUP NO RESPONSE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent NO_RESPONSE from eNodeB_CANDIDATE detected by CallpMgr.		
Remedial action: Check the behavior of the candidate eNodeB. If the alarm persists, check provisioning of the initiating and candidate eNodeBs.		

Table 29-504 IK4007028

Alarm	Attributes	Applicable major release
Name: IK4007028 (5225) Type: qualityOfServiceAlarm Package: lte.IK4007028 Raised on class: lte.Cell	Severity: indeterminate Specific problem: IMMEDIATE LOAD CONTROL END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicate that immediate load control procedure ends.		
Remedial action: No action is required.		

Table 29-505 IK4007045

Alarm	Attributes	Applicable major release
Name: IK4007045 (2549) Type: communicationsAlarm Package: lte.IK4007045 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB X2 SETUP REQ RESP FAIL UNKNOWN X2 ACCESS ID Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The eNodeB is implementing a check for future IOT. Common message like X2SAP X2 SETUP REQUEST/RESPONSE/FAILURE are received on a known X2 Access Id. If an unsolicited X2SAP X2 SETUP REQUEST message is received on an unknown X2 Access Id, the eNodeB answers with a X2SAP SETUP FAILURE and raises the event. If an unsolicited X2SAP X2 SETUP RESPONSE/FAILURE message is received on an unknown X2 ACCESS Id the eNodeB ignores the message and raises the event.		
Remedial action: No action is required.		

Table 29-506 IK4007046

Alarm	Attributes	Applicable major release
Name: IK4007046 (2550) Type: processingErrorAlarm Package: lte.IK4007046 Raised on class: lte.X2Access	Severity: major Specific problem: ANR X2IP ADDR RETRIEVAL FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the X2 IP address retrieval failure. When this alarm is raised, X2TransportLayerAccess is {Disabled, Failed} (and X2Access {Disabled, dependency}).		
Remedial action: Set the IP address manually.		

Table 29-507 IK4007052

Alarm	Attributes	Applicable major release
Name: IK4007052 (2552) Type: processingErrorAlarm Package: lte.IK4007052 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLTRACE ACTIVATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to activate a new trace recording session.		
Remedial action: No action is required.		

Table 29-508 IK4007053

Alarm	Attributes	Applicable major release
Name: IK4007053 (2553) Type: processingErrorAlarm Package: lte.IK4007053 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLTRACE SIGN TRACE STOPPED BY MGT TRACE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the signaling based trace session is stopped when eNodeB received a management based trace session activation request.		
Remedial action: No action is required.		

Table 29-509 IK4007054

Alarm	Attributes	Applicable major release
Name: IK4007054 (2554) Type: processingErrorAlarm Package: lte.IK4007054 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLTRACE COLLECTION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to collect trace data.		
Remedial action: No action is required.		

Table 29-510 IK4007055

Alarm	Attributes	Applicable major release
Name: IK4007055 (2555) Type: processingErrorAlarm Package: lte.IK4007055 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLTRACE INVALID PARAMETER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This even indicates the parameter received for call trace is invalid.		
Remedial action: No action is required.		

Table 29-511 IK4007056

Alarm	Attributes	Applicable major release
Name: IK4007056 (2556) Type: communicationsAlarm Package: lte.IK4007056 Raised on class: lte.Cell	Severity: major Specific problem: DSIM CELL AUTO BARRED Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-511 IK4007056 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the cell is auto-barred. If Dynamic Sysinfo Modification feature activated and MIM parameter LteCell.cellBarred set to 'notBarredAutoBarrable', the cell is auto-barred due to S1 service loss. This alarm is cleared when the cell is auto-unbarred due to S1 service recovery. When this alarm is raised, the related LteCell instance is {Enabled, Off-duty}.		
Remedial action: Resolve the S1 faults and restore S1 service.		

Table 29-512 IK4007057

Alarm	Attributes	Applicable major release
Name: IK4007057 (2557) Type: qualityOfServiceAlarm Package: lte.IK4007057 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: MME S1AP COMMON MESSAGE BAD ROUTING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the UeCallIp was routed a non-UE associated message.		
Remedial action: No action is required.		

Table 29-513 IK4007058

Alarm	Attributes	Applicable major release
Name: IK4007058 (2558) Type: qualityOfServiceAlarm Package: lte.IK4007058 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: MME S1AP DEDICATED MESSAGE BAD ROUTING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallPmgr was routed an UE associated message, that was therefore discarded.		
Remedial action: No action is required.		

Table 29-514 IK4007059

Alarm	Attributes	Applicable major release
Name: IK4007059 (2559) Type: communicationsAlarm Package: lte.IK4007059 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB X2AP MESSAGE MISMATCH Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the fault when X2AP message including 'served cell info' is received. CallP cross-checks in the MiM neighboring cells relating to a remote eNodeB with list of served cells received from the current eNodeB. This fault can be triggered upon reception of X2AP X2 SETUP REQUEST, X2AP X2 SETUP RESPONSE or X2AP ENB CONFIGURATION UPDATE. This event is not used when ANR is activated because the cross-check is not performed.		

Table 29-514 IK4007059 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-515 IK4007071

Alarm	Attributes	Applicable major release
Name: IK4007071 (2571) Type: processingErrorAlarm Package: lte.IK4007071 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 SYS INFO REFUSED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the BB L1/L2 entity rejected system information broadcast.		
Remedial action: 1 - lock the cell. 2- correct the wrong configuration value.\n3- unlock the cell.		

Table 29-516 IK4007072

Alarm	Attributes	Applicable major release
Name: IK4007072 (2572) Type: processingErrorAlarm Package: lte.IK4007072 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 SYS INFO TIMEOUT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a no-response from BB L1/L2 entity detected during the system information broadcast procedure.		
Remedial action: Lock and unlock the Cell. If the alarm persists, call the next level of support.		

Table 29-517 IK4007073

Alarm	Attributes	Applicable major release
Name: IK4007073 (2573) Type: processingErrorAlarm Package: lte.IK4007073 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CONFIG ERROR CELL SETUP Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a configuration error from BB L1/L2 entity detected during the Cell Setup procedure.		
Remedial action: Verify and correct the configuration data in the LTE CELL or CELL CONF.		

Table 29-518 IK4007074

Alarm	Attributes	Applicable major release
Name: IK4007074 (2574) Type: processingErrorAlarm Package: lte.IK4007074 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CELL SETUP REFUSED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the BB L1/L2 entity rejected the cell setup.		
Remedial action: Call the next level of support.		

Table 29-519 IK4007075

Alarm	Attributes	Applicable major release
Name: IK4007075 (2575) Type: processingErrorAlarm Package: lte.IK4007075 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CELL SETUP TIMEOUT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a no-response from BB L1/L2 entity detected during the Cell Setup procedure .		
Remedial action: Lock and unlock the cell. If the alarm persists, call the next level of support.		

Table 29-520 IK4007079

Alarm	Attributes	Applicable major release
Name: IK4007079 (2579) Type: processingErrorAlarm Package: lte.IK4007079 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CONFIG ERROR SYS INFO Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates configuration error from BB L1/L2 entity detected during system information broadcast.		
Remedial action: Verify and correct the configuration data in the LTE CELL or CELL CONF.		

Table 29-521 IK4007082

Alarm	Attributes	Applicable major release
Name: IK4007082 (2582) Type: processingErrorAlarm Package: lte.IK4007082 Raised on class: lte.Cell	Severity: warning Specific problem: L1L2 CONFIG MEAS FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-521 IK4007082 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that Measurement Configuration failed at L1/L2 entity level.		
Remedial action: Call the next level of support.		

Table 29-522 IK4007083

Alarm	Attributes	Applicable major release
Name: IK4007083 (2583) Type: operationalViolation Package: lte.IK4007083 Raised on class: lte.Cell	Severity: warning Specific problem: PCI COLLISION DETECTED UNDER RESOLUTION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI collision between the cell and a neighbour one. The eNodeB attempts for a resolution.		
Remedial action: If the alarm persists, call the next level of support.		

Table 29-523 IK4007084

Alarm	Attributes	Applicable major release
Name: IK4007084 (2584) Type: operationalViolation Package: lte.IK4007084 Raised on class: lte.Cell	Severity: critical Specific problem: PCI COLLISION DETECTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI collision between the cell and a neighbour one, or between the cell and another one of the same eNB. A manual intervention is needed to solve the problem. This can happen in the following cases: - The conflict could not be solved autonomously by\nthe eNB; - The automatic PCI allocation is not activated		
Remedial action: Increase the list of allowed PCI values, either for the local or for the distant eNodeB when the other contributor is distant.		

Table 29-524 IK4007085

Alarm	Attributes	Applicable major release
Name: IK4007085 (2585) Type: operationalViolation Package: lte.IK4007085 Raised on class: lte.Cell	Severity: warning Specific problem: PCI CONFUSION DETECTED UNDER RESOLUTION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI confusion between the cell and a neighbour one. The eNodeB attempts for a resolution.		

Table 29-524 IK4007085 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the alarm persists, call the next level of support.		

Table 29-525 IK4007088

Alarm	Attributes	Applicable major release
Name: IK4007088 (2588) Type: qualityOfServiceAlarm Package: lte.IK4007088 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB X2 COMMON MESSAGE BAD ROUTING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a X2-AP non-UE associated message is routed to UeCallP.		
Remedial action: No action is required.		

Table 29-526 IK4007089

Alarm	Attributes	Applicable major release
Name: IK4007089 (2589) Type: qualityOfServiceAlarm Package: lte.IK4007089 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB X2 DEDICATED MESSAGE BAD ROUTING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a X2-AP UE associated message is routed to CallPMgr.		
Remedial action: No action is required.		

Table 29-527 IK4007091

Alarm	Attributes	Applicable major release
Name: IK4007091 (2590) Type: operationalViolation Package: lte.IK4007091 Raised on class: lte.Cell	Severity: critical Specific problem: PCI DETECTION OF INTERFERENCE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the PCI interference.		
Remedial action: Increase the list of allowed PCI values for the serving eNodeB. The eNodeB must be able to allocate PCIs that are different modulo 3 for its cells (or for a cell and 2 co-sector cells), so the 3 values of PCI mod 3 must be present in the list of allowed PCI values. In case all the cells of a site raise an Interference alarm, check the configuration as it may inform about a site configuration error (too many cells in a site, wrong omni or cell azimuth in a site).		

Table 29-528 IK4007093

Alarm	Attributes	Applicable major release
Name: IK4007093 (2592) Type: communicationsAlarm Package: lte.IK4007093 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ANR SERVED CELL INFO NOT HANDLED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the served cell and neighbor cell information received over X2 interface is not handled, because internal eNodeB tables reached the dimensioning limits.		
Remedial action: No action is required.		

Table 29-529 IK4007094

Alarm	Attributes	Applicable major release
Name: IK4007094 (2593) Type: communicationsAlarm Package: lte.IK4007094 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB CANDIDATE X2 ENB CONFIGURATION UPDATE FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent X2_ENB_CONFIGURATION_UPDATE _FAILURE message from eNB_Candidate eNodeB2 network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-530 IK4007095

Alarm	Attributes	Applicable major release
Name: IK4007095 (2594) Type: communicationsAlarm Package: lte.IK4007095 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB CANDIDATE X2 ENB CONFIGURATION UPDATE NO RESPONSE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent NO_RESPONSE from eNodeB_CANDIDATE eNodeB2 network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-531 IK4007096

Alarm	Attributes	Applicable major release
Name: IK4007096 (2595) Type: qualityOfServiceAlarm Package: lte.IK4007096 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: MME S1 ENB CONFIGURATION UPDATE FAILURE RESPONSE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent S1_ENB_CONFIGURATION_UPDATE_FAILURE_RESPONSE from MME network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-532 IK4007097

Alarm	Attributes	Applicable major release
Name: IK4007097 (2596) Type: qualityOfServiceAlarm Package: lte.IK4007097 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: MME S1 ENB CONFIGURATION UPDATE NO RESPONSE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent NO_RESPONSE from MME network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-533 IK4007098

Alarm	Attributes	Applicable major release
Name: IK4007098 (2597) Type: communicationsAlarm Package: lte.IK4007098 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: INCONSISTENT IP ADDRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the IP address attached to X2TransportLayerAccess instance depending on the X2Access instance is not correct.		
Remedial action: No action is required.		

Table 29-534 IK4007099

Alarm	Attributes	Applicable major release
Name: IK4007099 (2598) Type: communicationsAlarm Package: lte.IK4007099 Raised on class: lte.BscAccess	Severity: minor Specific problem: GERAN SYS INFO TRANSFER INITIATION REPORT FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that CallP does not manage to retrieve the system information (SI/PSI) of a target GERAN cell using RIM RAN-INFORMATION-REQUEST/multiple report.		
Remedial action: Check for the proper functioning of the following:1. GERAN cell provisioning;2. RIM support for MME and SGSN;3. IP routing path between eNodeB S1 interface IP endpoint and target BSC.		

Table 29-535 IK4007100

Alarm	Attributes	Applicable major release
Name: IK4007100 (2599) Type: communicationsAlarm Package: lte.IK4007100 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: GERAN SYS INFO TRANSFER STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallP does not manage to stop event-driven system information (SI/PSI) of a target GERAN Cell using RIM RAN-INFORMATION-REQUEST/stop.		
Remedial action: No action is required.		

Table 29-536 IK4007101

Alarm	Attributes	Applicable major release
Name: IK4007101 (2600) Type: communicationsAlarm Package: lte.IK4007101 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: GERAN SYS INFO UPDATE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB CallP has received RIM RAN-INFORMATION/end message from a target BSC indicating that event-driven system information update for a target GERAN cell has been stopped.		
Remedial action: No action is required.		

Table 29-537 IK4007102

Alarm	Attributes	Applicable major release
Name: IK4007102 (2601) Type: communicationsAlarm Package: lte.IK4007102 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: RAN INFORMATION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that there is an error in RIM container IE when eNodeB receive RIM message from peer node or RAN-INFORMATION-ERROR message is received from peer node.		
Remedial action: No action is required.		

Table 29-538 IK4007103

Alarm	Attributes	Applicable major release
Name: IK4007103 (2602) Type: communicationsAlarm Package: lte.IK4007103 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: RAN INFORMATION APPLICATION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates there is an error in application container IE or there is application error container IE when eNodeB receive RIM message from peer node.		
Remedial action: No action is required.		

Table 29-539 IK4007104

Alarm	Attributes	Applicable major release
Name: IK4007104 (2603) Type: qualityOfServiceAlarm Package: lte.IK4007104 Raised on class: lte.Cell	Severity: critical Specific problem: CELL SETUP ARP TIMEOUT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a non-response to an ARP resolution request detected during the Cell Setup procedure.		
Remedial action: Call the next level of support.		

Table 29-540 IK4007105

Alarm	Attributes	Applicable major release
Name: IK4007105 (2604) Type: processingErrorAlarm Package: lte.IK4007105 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: L1L2 CONFIG REFUSED CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates the cell deletion for logical cell resetting procedure is rejected by the BB entity.		
Remedial action: Lock then unlock the BB.		

Table 29-541 IK4007106

Alarm	Attributes	Applicable major release
Name: IK4007106 (2605) Type: processingErrorAlarm Package: lte.IK4007106 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: L1L2 CONFIG TIMEOUT CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a non-response from BB entity for cell deletion in the logical cell resetting procedure.		
Remedial action: Lock then unlock the BB.		

Table 29-542 IK4007107

Alarm	Attributes	Applicable major release
Name: IK4007107 (2606) Type: processingErrorAlarm Package: lte.IK4007107 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: CELL CLEAN UP FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a cell deletion failure when cell clean-up is triggered by LteCell instance deletion online, parameter update or when software failure happens		
Remedial action: Lock then unlock the BB.		

Table 29-543 IK4007108

Alarm	Attributes	Applicable major release
Name: IK4007108 (2607) Type: communicationsAlarm Package: lte.IK4007108 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: ENB X2 PLMN INCONSISTENCY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates an inconsistency between the PLMN ID of Global eNB ID, Served Cell Information or Neighbour Information received from candidate eNB in X2AP message (X2 SETUP REQUEST, X2 SETUP RESPONSE, ENB CONFIGURATION UPDATE) and local eNodeB's PLMN ID.		
Remedial action: No action is required.		

Table 29-544 IK4007109

Alarm	Attributes	Applicable major release
Name: IK4007109 (2608) Type: processingErrorAlarm Package: lte.IK4007109 Raised on class: lte.Cell	Severity: major Specific problem: L1L2 CONFIG ERROR CELL UPDATE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a configuration error detected by BB entity for the cell update procedure.		
Remedial action: Check and correct the wrong parameter.		

Table 29-545 IK4007110

Alarm	Attributes	Applicable major release
Name: IK4007110 (2609) Type: processingErrorAlarm Package: lte.IK4007110 Raised on class: lte.Cell	Severity: major Specific problem: L1L2 CONFIG REFUSED CELL UPDATE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a cell update is refused by the BB entity.		
Remedial action: Call the next level of support.		

Table 29-546 IK4007111

Alarm	Attributes	Applicable major release
Name: IK4007111 (2610) Type: processingErrorAlarm Package: lte.IK4007111 Raised on class: lte.Cell	Severity: major Specific problem: L1L2 CONFIG TIMEOUT CELL UPDATE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a non-response by the BB entity to the cell update procedure.		
Remedial action: Lock and unlock the cell. If the alarm persists. Call the next level of support.		

Table 29-547 IK4007112

Alarm	Attributes	Applicable major release
Name: IK4007112 (2611) Type: communicationsAlarm Package: lte.IK4007112 Raised on class: lte.MmeAccess	Severity: critical Specific problem: MME S1 SETUP REQUEST NOT SENT Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the S1 Setup Request has not been sent because of an internal problem.		
Remedial action: Check the parameters.		

Table 29-548 IK4007113

Alarm	Attributes	Applicable major release
Name: IK4007113 (2612) Type: processingErrorAlarm Package: lte.IK4007113 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CONFIG ERROR CELL MBMS SCHEDULING INFO Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the Cell MBMS scheduling info is rejected by the BB entity because of a configuration error.		
Remedial action: Check the parameters.		

Table 29-549 IK4007114

Alarm	Attributes	Applicable major release
Name: IK4007114 (2613) Type: processingErrorAlarm Package: lte.IK4007114 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CONFIG REFUSED CELL MBMS SCHEDULING INFO Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the Cell MBMS scheduling info is refused by the BB entity.		
Remedial action: Call the next level of support.		

Table 29-550 IK4007115

Alarm	Attributes	Applicable major release
Name: IK4007115 (2614) Type: processingErrorAlarm Package: lte.IK4007115 Raised on class: lte.Cell	Severity: critical Specific problem: L1L2 CONFIG TIMEOUT CELL MBMS SCHEDULING INFO Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a non-response by the BB entity to the Cell MBMS scheduling info procedure.		
Remedial action: Call the next level of support.		

Table 29-551 IK4007116

Alarm	Attributes	Applicable major release
Name: IK4007116 (2615) Type: processingErrorAlarm Package: lte.IK4007116 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB DELAY CONFIG FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a modification of delays requiring BB to be reset so to use new values.		
Remedial action: Reset the BB.		

Table 29-552 IK4007117

Alarm	Attributes	Applicable major release
Name: IK4007117 (3058) Type: processingErrorAlarm Package: lte.IK4007117 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CALLTRACE SIGN BASED STOPPED BY DDT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the signaling based trace session is stopped when eNodeB received a dynamic debug trace session activation request.		
Remedial action: No action is required.		

Table 29-553 IK4007118

Alarm	Attributes	Applicable major release
Name: IK4007118 (3059) Type: processingErrorAlarm Package: lte.IK4007118 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DYNAMIC DEBUG TRACE ACTIVATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the dynamic debug trace activation failed.		
Remedial action: No action is required.		

Table 29-554 IK4007119

Alarm	Attributes	Applicable major release
Name: IK4007119 (3060) Type: processingErrorAlarm Package: lte.IK4007119 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DYNAMIC DEBUG TRACE INVALID PARAMETER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the dynamic debug trace parameters are invalid.		
Remedial action: No action is required.		

Table 29-555 IK4007120

Alarm	Attributes	Applicable major release
Name: IK4007120 (3061) Type: communicationsAlarm Package: lte.IK4007120 Raised on class: lte.Cell	Severity: major Specific problem: NO RRC CONNECTIONS DETECTED FOR A PERIOD Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that no RRC connection has been setup for a period (no new connections, no re-establishments and no incoming handovers). This period is configurable per Cell.		
Remedial action: Check the configurable period and the hours this alarm is raised. If configurable period is long enough such that some connections should have been established, please call the next level of support.		

Table 29-556 IK4007121

Alarm	Attributes	Applicable major release
Name: IK4007121 (3062) Type: processingErrorAlarm Package: lte.IK4007121 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-557 IK4007122

Alarm	Attributes	Applicable major release
Name: IK4007122 (3063) Type: processingErrorAlarm Package: lte.IK4007122 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-558 IK4007123

Alarm	Attributes	Applicable major release
Name: IK4007123 (3064) Type: processingErrorAlarm Package: lte.IK4007123 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-559 IK4007124

Alarm	Attributes	Applicable major release
Name: IK4007124 (3065) Type: processingErrorAlarm Package: lte.IK4007124 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified BB fault detected		
Remedial action: No action is required.		

Table 29-560 IK4007125

Alarm	Attributes	Applicable major release
Name: IK4007125 (3066) Type: processingErrorAlarm Package: lte.IK4007125 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified BB fault detected		
Remedial action: No action is required.		

Table 29-561 IK4007126

Alarm	Attributes	Applicable major release
Name: IK4007126 (3067) Type: processingErrorAlarm Package: lte.IK4007126 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-561 IK4007126 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in.\nUnspecified BB fault detected		
Remedial action: No action is required.		

Table 29-562 IK4007127

Alarm	Attributes	Applicable major release
Name: IK4007127 (3068) Type: processingErrorAlarm Package: lte.IK4007127 Raised on class: lte.BscAccess	Severity: minor Specific problem: BSC_ACCESS FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BSC Access fault		
Remedial action: Check the additional information for maintenance action details.		

Table 29-563 IK4007128

Alarm	Attributes	Applicable major release
Name: IK4007128 (3069) Type: processingErrorAlarm Package: lte.IK4007128 Raised on class: lte.BscAccess	Severity: minor Specific problem: BSC_ACCESS FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BSC Access fault		
Remedial action: Check the additional information for maintenance action details.		

Table 29-564 IK4007129

Alarm	Attributes	Applicable major release
Name: IK4007129 (3070) Type: processingErrorAlarm Package: lte.IK4007129 Raised on class: lte.BscAccess	Severity: minor Specific problem: BSC_ACCESS FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BSC Access fault		
Remedial action: Check the additional information for maintenance action details.		

Table 29-565 IK4007130

Alarm	Attributes	Applicable major release
Name: IK4007130 (3071) Type: processingErrorAlarm Package: lte.IK4007130 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: BSC_ACCESS EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-566 IK4007131

Alarm	Attributes	Applicable major release
Name: IK4007131 (3072) Type: processingErrorAlarm Package: lte.IK4007131 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: BSC_ACCESS EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-567 IK4007132

Alarm	Attributes	Applicable major release
Name: IK4007132 (3073) Type: processingErrorAlarm Package: lte.IK4007132 Raised on class: lte.BscAccess	Severity: indeterminate Specific problem: BSC_ACCESS EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-568 IK4007135

Alarm	Attributes	Applicable major release
Name: IK4007135 (3076) Type: processingErrorAlarm Package: lte.IK4007135 Raised on class: lte.Cell	Severity: minor Specific problem: CELL FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified Cell fault.		

Table 29-568 IK4007135 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the additional information for maintenance action details.		

Table 29-569 IK4007136

Alarm	Attributes	Applicable major release
Name: IK4007136 (3077) Type: processingErrorAlarm Package: lte.IK4007136 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-570 IK4007137

Alarm	Attributes	Applicable major release
Name: IK4007137 (3078) Type: processingErrorAlarm Package: lte.IK4007137 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-571 IK4007138

Alarm	Attributes	Applicable major release
Name: IK4007138 (3079) Type: processingErrorAlarm Package: lte.IK4007138 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-572 IK4007139

Alarm	Attributes	Applicable major release
Name: IK4007139 (3080) Type: processingErrorAlarm Package: lte.IK4007139 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ENB FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified eNodeB fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-573 IK4007140

Alarm	Attributes	Applicable major release
Name: IK4007140 (3081) Type: processingErrorAlarm Package: lte.IK4007140 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ENB FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified eNodeB fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-574 IK4007141

Alarm	Attributes	Applicable major release
Name: IK4007141 (3082) Type: processingErrorAlarm Package: lte.IK4007141 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ENB FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified eNodeB fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-575 IK4007144

Alarm	Attributes	Applicable major release
Name: IK4007144 (3085) Type: processingErrorAlarm Package: lte.IK4007144 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-575 IK4007144 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the maximum number of object cardinality is reached. The automatic creation of new objects is not possible anymore.		
Remedial action: No action is required.		

Table 29-576 IK4007145

Alarm	Attributes	Applicable major release
Name: IK4007145 (3086) Type: processingErrorAlarm Package: lte.IK4007145 Raised on class: lte.MmeAccess	Severity: minor Specific problem: S1 FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified S1 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-577 IK4007146

Alarm	Attributes	Applicable major release
Name: IK4007146 (3087) Type: processingErrorAlarm Package: lte.IK4007146 Raised on class: lte.MmeAccess	Severity: minor Specific problem: S1 FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified S1 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-578 IK4007147

Alarm	Attributes	Applicable major release
Name: IK4007147 (3088) Type: processingErrorAlarm Package: lte.IK4007147 Raised on class: lte.MmeAccess	Severity: minor Specific problem: S1 FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified S1 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-579 IK4007148

Alarm	Attributes	Applicable major release
Name: IK4007148 (3089) Type: processingErrorAlarm Package: lte.IK4007148 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: S1 EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-580 IK4007149

Alarm	Attributes	Applicable major release
Name: IK4007149 (3090) Type: processingErrorAlarm Package: lte.IK4007149 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: S1 EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-581 IK4007150

Alarm	Attributes	Applicable major release
Name: IK4007150 (3091) Type: processingErrorAlarm Package: lte.IK4007150 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: S1 EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-582 IK4007151

Alarm	Attributes	Applicable major release
Name: IK4007151 (3092) Type: processingErrorAlarm Package: lte.IK4007151 Raised on class: lte.X2Access	Severity: minor Specific problem: X2 FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-582 IK4007151 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified X2 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-583 IK4007152

Alarm	Attributes	Applicable major release
Name: IK4007152 (3093) Type: processingErrorAlarm Package: lte.IK4007152 Raised on class: lte.X2Access	Severity: minor Specific problem: X2 FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified X2 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-584 IK4007153

Alarm	Attributes	Applicable major release
Name: IK4007153 (3094) Type: processingErrorAlarm Package: lte.IK4007153 Raised on class: lte.X2Access	Severity: minor Specific problem: X2 FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified X2 fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-585 IK4007154

Alarm	Attributes	Applicable major release
Name: IK4007154 (3095) Type: processingErrorAlarm Package: lte.IK4007154 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: X2 EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-586 IK4007155

Alarm	Attributes	Applicable major release
Name: IK4007155 (3096) Type: processingErrorAlarm Package: lte.IK4007155 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: X2 EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-587 IK4007156

Alarm	Attributes	Applicable major release
Name: IK4007156 (3097) Type: processingErrorAlarm Package: lte.IK4007156 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: X2 EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-588 IK4007157

Alarm	Attributes	Applicable major release
Name: IK4007157 (3098) Type: processingErrorAlarm Package: lte.IK4007157 Raised on class: lte.UtraFddNeighboringFreqConf	Severity: indeterminate Specific problem: END OF INTERRAT UTRAN ANR ACTIVE PHASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the inter-RAT UTRAN ANR active phase.		
Remedial action: No action is required.		

Table 29-589 IK4007159

Alarm	Attributes	Applicable major release
Name: IK4007159 (3100) Type: processingErrorAlarm Package: lte.IK4007159 Raised on class: lte.UtraFddNeighboringCellRelation	Severity: indeterminate Specific problem: CREATED UTRAN NEIGHBOR CANNOT BE ASSOCIATED TO RNC Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-589 IK4007159 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates no RNC is found to associate the UtraFddNeighbouringCellRelation.		
Remedial action: No action is required.		

Table 29-590 IK4007160

Alarm	Attributes	Applicable major release
Name: IK4007160 (3101) Type: communicationsAlarm Package: lte.IK4007160 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: END CMAS ALERT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the CMAS message broadcast.		
Remedial action: No action is required.		

Table 29-591 IK4007161

Alarm	Attributes	Applicable major release
Name: IK4007161 (3102) Type: processingErrorAlarm Package: lte.IK4007161 Raised on class: lte.Cell	Severity: indeterminate Specific problem: L1L2 CONFIG REFUSED CMAS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the BB L1/L2 entity rejected CMAS message broadcast.		
Remedial action: No action is required.		

Table 29-592 IK4007162

Alarm	Attributes	Applicable major release
Name: IK4007162 (3103) Type: processingErrorAlarm Package: lte.IK4007162 Raised on class: lte.Cell	Severity: indeterminate Specific problem: L1L2 CONFIG TIMEOUT CMAS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a no-response from BB L1/L2 entity detected during the CMAS broadcast procedure.		
Remedial action: No action is required.		

Table 29-593 IK4007163

Alarm	Attributes	Applicable major release
Name: IK4007163 (3104) Type: communicationsAlarm Package: lte.IK4007163 Raised on class: lte.RncAccess	Severity: minor Specific problem: UTRAN SYS INFO TRANSFER INITIATION REPORT FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that CallP does not manage to retrieve the system information (UTRASI) of a target UTRAN cell using RIM RAN-INFORMATION-REQUEST/multiple report.		
Remedial action: Check for the proper functioning of the following:\n1. UTRAN cell provisioning\n2. RIM support for MME and SGSN\n3. IP routing path between eNodeB S1 interface IP endpoint and target RNC.		

Table 29-594 IK4007164

Alarm	Attributes	Applicable major release
Name: IK4007164 (3105) Type: communicationsAlarm Package: lte.IK4007164 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRAN SYS INFO UPDATE STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallP does not manage to stop event-driven system information (UTRASI) of a target UTRAN Cell using RIM RAN-INFORMATION-REQUEST/stop.		
Remedial action: No action is required.		

Table 29-595 IK4007165

Alarm	Attributes	Applicable major release
Name: IK4007165 (3106) Type: communicationsAlarm Package: lte.IK4007165 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRAN SYS INFO UPDATE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB CallP has received RIM RAN-INFORMATION/end message from a target RNC indicating that event-driven system information update for a target UTRAN cell has been stopped.		
Remedial action: No action is required.		

Table 29-596 IK4007166

Alarm	Attributes	Applicable major release
Name: IK4007166 (3107) Type: communicationsAlarm Package: lte.IK4007166 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRA RAN INFORMATION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that there is an error in RIM container IE when eNodeB receive RIM message from peer node or RAN-INFORMATION-ERROR message is received from peer node.		
Remedial action: No action is required.		

Table 29-597 IK4007167

Alarm	Attributes	Applicable major release
Name: IK4007167 (3108) Type: communicationsAlarm Package: lte.IK4007167 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRA RAN INFORMATION APPLICATION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates there is an error in application container IE or there is application error container IE when eNodeB receive RIM message from peer node.		
Remedial action: No action is required.		

Table 29-598 IK4007169

Alarm	Attributes	Applicable major release
Name: IK4007169 (3110) Type: processingErrorAlarm Package: lte.IK4007169 Raised on class: lte.Cell	Severity: indeterminate Specific problem: END OF INTRAFREQ LTE ANR ACTIVE PHASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the intra-frequency LTE ANR active phase.		
Remedial action: No action is required.		

Table 29-599 IK4007170

Alarm	Attributes	Applicable major release
Name: IK4007170 (3111) Type: qualityOfServiceAlarm Package: lte.IK4007170 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: MME S1 SETUP RESPONSE INCONSISTENCY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a configuration mismatch between the MIM and the MME.		
Remedial action: No action is required.		

Table 29-600 IK4007171

Alarm	Attributes	Applicable major release
Name: IK4007171 (3780) Type: communicationsAlarm Package: lte.IK4007171 Raised on class: lte.X2Access	Severity: minor Specific problem: X2 RESOURCE STATUS REPORTING INITIATION FAILURE OR NO RESPONSE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent X2AP RESOURCE STATUS FAILURE message or no response from a peer eNodeB.		
Remedial action: Check peer eNB and do X2 lock/unlock when it is available for X2 load reporting		

Table 29-601 IK4007172

Alarm	Attributes	Applicable major release
Name: IK4007172 (3781) Type: processingErrorAlarm Package: lte.IK4007172 Raised on class: lte.Cell	Severity: indeterminate Specific problem: END OF INTER-FREQ ANR ACTIVE PHASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the inter-frequency LTE ANR active phase.		
Remedial action: No action is required.		

Table 29-602 IK4007175

Alarm	Attributes	Applicable major release
Name: IK4007175 (3782) Type: processingErrorAlarm Package: lte.IK4007175 Raised on class: lte.Cell	Severity: indeterminate Specific problem: SIB3 AUTOMATED PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the cell has automatically modified cell reselection parameters broadcast in SIB3 based on cell loading conditions		
Remedial action: No action is required.		

Table 29-603 IK4007176

Alarm	Attributes	Applicable major release
Name: IK4007176 (3783) Type: securityServiceOrMechanismViolation Package: lte.IK4007176 Raised on class: lte.Cell	Severity: indeterminate Specific problem: SIB RATE EXCESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that SIB updates incremented the Value Tag more than 32 times in elapsed 3 hours.		
Remedial action: No action is required.		

Table 29-604 IK4007177

Alarm	Attributes	Applicable major release
Name: IK4007177 (3784) Type: qualityOfServiceAlarm Package: lte.IK4007177 Raised on class: lte.Cell	Severity: major Specific problem: EMBMS QOS Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that eMBMS service is experiencing packet loss (greater than LteCell::mbmsPacketLossThrHigh) or excessive delay (packets are detected in excess in eMBMS buffers).		
Remedial action: Depending on the reason found different actions can be taken: (1)packet loss or delay between the eNB and the BM-SC: fix network issue; (2) estimated network delay in the BM-SC is not correct: Check the network delay at the BM-SC; (3) time reference is different in eNB and BM-SC: check the synchronization period and the synchronization sequence provisionned in the BM-SC and the eNB parameters Mbms::m1SyncSequenceDuration and m1SyncPeriodDuration. The Mbms::m1SyncPeriodOffset can also be set on the eNB side to make a correction on the time-stamps received from the BM-SC. This value is subtracted to the BM-SC time-stamp (modulus m1SyncPeriodDuration). The same value shall be set on all eNBs of a MBSFN area. When possible, it is preffered to adjust the delay directly in the BM-SC rather than setting the syncPeriodOffset. (4) mismatch between the service bit rate and the resources allocated in the eNB: check MCE and content provider provisionning: the effective bit rate on the M1 interface seems to exceed the bit rate announced in M3 session start. (5) the status of the synchronization clock source.		

Table 29-605 IK4007179

Alarm	Attributes	Applicable major release
Name: IK4007179 (3786) Type: processingErrorAlarm Package: lte.IK4007179 Raised on class: lte.Cell	Severity: critical Specific problem: CELL DISABLED DUE TO BAD POWER CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the LTE Cell is disabled due to misconfiguration in power settings during cell setup procedure or cell parameter update procedure.		
Remedial action: Correct the LteCell power parameters configuration and apply the update , and then perform lock/unlock cell so to put the LteCell back into service.		

Table 29-606 IK4007183

Alarm	Attributes	Applicable major release
Name: IK4007183 (3789) Type: qualityOfServiceAlarm Package: lte.IK4007183 Raised on class: lte.Cell	Severity: indeterminate Specific problem: INCOMPLETE BROADCAST OF A PRESIDENTIAL ALERT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNB has been unable to broadcast a CMAS Presidential Alert the requested number of times.		
Remedial action: No action is required.		

Table 29-607 IK4007184

Alarm	Attributes	Applicable major release
Name: IK4007184 (3989) Type: processingErrorAlarm Package: lte.IK4007184 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BRC UC FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the UeCallIP detected a no-response from BRC-UC.		
Remedial action: No action is required.		

Table 29-608 IK4007185

Alarm	Attributes	Applicable major release
Name: IK4007185 (3990) Type: processingErrorAlarm Package: lte.IK4007185 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BRC UC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BRC-UC reported a warning.		
Remedial action: No action is required.		

Table 29-609 IK4007188

Alarm	Attributes	Applicable major release
Name: IK4007188 (4657) Type: processingErrorAlarm Package: lte.IK4007188 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BRC CC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BRC-CC reported a warning.		
Remedial action: No action is required.		

Table 29-610 IK4007189

Alarm	Attributes	Applicable major release
Name: IK4007189 (4658) Type: processingErrorAlarm Package: lte.IK4007189 Raised on class: lte.MODULE	Severity: major Specific problem: L1L2 CONFIG REFUSED CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates the cell deletion for logical cell resetting procedure is rejected by the Modem entity.		
Remedial action: Lock then unlock the eNB		

Table 29-611 IK4007190

Alarm	Attributes	Applicable major release
Name: IK4007190 (4659) Type: processingErrorAlarm Package: lte.IK4007190 Raised on class: lte.MODULE	Severity: major Specific problem: L1L2 CONFIG TIMEOUT CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L

Table 29-611 IK4007190 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a lack of response from the modem for cell deletion in the logical cell resetting procedure.		
Remedial action: Lock then unlock the eNB.		

Table 29-612 IK4007191

Alarm	Attributes	Applicable major release
Name: IK4007191 (4660) Type: processingErrorAlarm Package: lte.IK4007191 Raised on class: lte.MODULE	Severity: major Specific problem: CELL CLEAN UP FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a cell deletion failure when cell clean-up is triggered by LteCell instance deletion online, parameter update or when software failure happens.		
Remedial action: Lock then unlock the eNB.		

Table 29-613 IK4007192

Alarm	Attributes	Applicable major release
Name: IK4007192 (4661) Type: processingErrorAlarm Package: lte.IK4007192 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB DELAY CONFIG FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: Configured cell path delays are no longer correct and the modem function must be reset to adopt the new values.		
Remedial action: Reset the modem.		

Table 29-614 IK4007196

Alarm	Attributes	Applicable major release
Name: IK4007196 (4665) Type: processingErrorAlarm Package: lte.IK4007196 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified Modem Function fault detected		
Remedial action: No action is required.		

Table 29-615 IK4007197

Alarm	Attributes	Applicable major release
Name: IK4007197 (4666) Type: processingErrorAlarm Package: lte.IK4007197 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified Modem Function fault detected		
Remedial action: No action is required.		

Table 29-616 IK4007198

Alarm	Attributes	Applicable major release
Name: IK4007198 (4667) Type: processingErrorAlarm Package: lte.IK4007198 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified Modem Function fault detected		
Remedial action: No action is required.		

Table 29-617 IK4007201

Alarm	Attributes	Applicable major release
Name: IK4007201 (4668) Type: processingErrorAlarm Package: lte.IK4007201 Raised on class: lte.ENBEquipment	Severity: major Specific problem: ANR X2IP ADDR RETRIEVAL FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the X2 IP address retrieval failure. The alarm is cleared when X2Access instance created or internal timer.		
Remedial action: Create the X2Access instance, if an X2 link needs to be established.		

Table 29-618 IK4007202

Alarm	Attributes	Applicable major release
Name: IK4007202 (4669) Type: processingErrorAlarm Package: lte.IK4007202 Raised on class: lte.Cell	Severity: indeterminate Specific problem: NEIGHBOR RELATION REPLACEMENT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-618 IK4007202 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that a Neighbor Relation has been replaced with another higher priority neighbor.		
Remedial action: No action is required.		

Table 29-619 IK4007204

Alarm	Attributes	Applicable major release
Name: IK4007204 (4671) Type: communicationsAlarm Package: lte.IK4007204 Raised on class: lte.RncAccess	Severity: minor Specific problem: UTRAN CELL LOAD TRANSFER INITIATION REPORT FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that CallP does not manage to retrieve the cell load of a target UTRAN cell using RIM RAN-INFORMATION-REQUEST/multiple report.		
Remedial action: Check for the proper functioning of the following:1. UTRAN cell provisioning; 2. RIM support for MME and SGSN; 3. IP routing path between eNodeB S1 interface IP endpoint and target RNC.		

Table 29-620 IK4007206

Alarm	Attributes	Applicable major release
Name: IK4007206 (4673) Type: operationalViolation Package: lte.IK4007206 Raised on class: lte.MmeAccess	Severity: critical Specific problem: SCTP RELEASE DUE TO DUPLICATED MMECs Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a MMEC or PLMN, MMEGI, MMEC in the 'Served GUMMEIs' IE of S1 Setup Response from one MME was found to be a duplicate with the existing ones from another MME.		
Remedial action: Update MMEGI or MMEC to make MMEGI, MMEC unique across all MMEs having SCTP with the eNodeB, and then re-try S1 Setup.		

Table 29-621 IK4007207

Alarm	Attributes	Applicable major release
Name: IK4007207 (4674) Type: communicationsAlarm Package: lte.IK4007207 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRAN CELL LOAD TRANSFER STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-621 IK4007207 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that CallP does not manage to stop event-driven cell load exchange of a target UTRAN Cell using RIM RAN-INFORMATION-REQUEST/stop.		
Remedial action: No action is required.		

Table 29-622 IK4007208

Alarm	Attributes	Applicable major release
Name: IK4007208 (4675) Type: communicationsAlarm Package: lte.IK4007208 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: UTRAN CELL LOAD UPDATE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB CallP has received RIM RAN-INFORMATION/end message from a target RNC indicating that event-driven cell load update for a target UTRAN cell has been stopped.		
Remedial action: No action is required.		

Table 29-623 IK4007212

Alarm	Attributes	Applicable major release
Name: IK4007212 (7973) Type: qualityOfServiceAlarm Package: lte.IK4007212 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ABS DUTY CYCLE IMPACT ON DL PRB CONSUMPTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that an on-line change of the ABS duty cycle leads to increase the downlink percentage of the PRB consumption beyond a configurable threshold called eIcicDlAlarmOnAbsDutyCycleThresholdOnPrb in the object called eIcicAbsGenerationConf.		
Remedial action: No action is required.		

Table 29-624 IK4007214

Alarm	Attributes	Applicable major release
Name: IK4007214 (7974) Type: processingErrorAlarm Package: lte.IK4007214 Raised on class: lte.Cell	Severity: indeterminate Specific problem: END OF INTERRAT CDMA HRPD ANR ACTIVE PHASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the inter-RAT CDMA HRPD ANR active phase.		

Table 29-624 IK4007214 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-625 IK4007215

Alarm	Attributes	Applicable major release
Name: IK4007215 (7975) Type: processingErrorAlarm Package: lte.IK4007215 Raised on class: lte.Cell	Severity: indeterminate Specific problem: END OF INTERRAT CDMA 1xRTT ANR ACTIVE PHASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the end of the inter-RAT CDMA 1xRTT ANR active phase.		
Remedial action: No action is required.		

Table 29-626 IK4007218

Alarm	Attributes	Applicable major release
Name: IK4007218 (7978) Type: processingErrorAlarm Package: lte.IK4007218 Raised on class: lte.Cell	Severity: indeterminate Specific problem: HRPD NEIGHBOR RELATION REPLACEMENT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a HRPD Neighbor Relation has been replaced with another higher priority neighbor.		
Remedial action: No action is required.		

Table 29-627 IK4007219

Alarm	Attributes	Applicable major release
Name: IK4007219 (7979) Type: processingErrorAlarm Package: lte.IK4007219 Raised on class: lte.Cell	Severity: indeterminate Specific problem: 1xRTT NEIGHBOR RELATION REPLACEMENT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a 1xRTT Neighbor Relation has been replaced with another higher priority neighbor.		
Remedial action: No action is required.		

Table 29-628 IK4007220

Alarm	Attributes	Applicable major release
Name: IK4007220 (7980) Type: operationalViolation Package: lte.IK4007220 Raised on class: lte.Cell	Severity: major Specific problem: PCI CONFUSION CDMA NEIGHB CELLS Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates this cell is a victim of a CDMA PCI (pnOffset) confusion, it has neighbor cells in a particular CDMA neighboring frequency that have the same PCI. A manual intervention is needed to solve the problem. This issue may affect mobility procedures from LTE to CDMA.		
Remedial action: The maintenance action is to change the PCI value of one of the neighbor CDMA cells to resolve the conflict.		

Table 29-629 IK4007221

Alarm	Attributes	Applicable major release
Name: IK4007221 (7981) Type: processingErrorAlarm Package: lte.IK4007221 Raised on class: lte.UtraFddNeighboringCellRelation	Severity: major Specific problem: UTRAN NEIGHBOR RELATION MIB INSTANCE CANNOT BE REMOVED BY ANR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the UTRAN neighbor relation MIB instance is not removed because the removal is not allowed.		
Remedial action: Remove the existing UTRAN neighbor relation so that it can be created by ANR under the correct frequency.		

Table 29-630 IK4007222

Alarm	Attributes	Applicable major release
Name: IK4007222 (7982) Type: operationalViolation Package: lte.IK4007222 Raised on class: lte.Cell	Severity: warning Specific problem: PCI OUT OF PCI ALLOWED LIST DETECTED UNDER RESOLUTION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI out of the related pciAllowedList provided by the operator. The eNodeB attempts for a resolution.		
Remedial action: This is due to an operator action. AutoPCI will solve the issue by changing the PCI. So check that pciAllowedList is the one that you really need.		

Table 29-631 IK4007223

Alarm	Attributes	Applicable major release
Name: IK4007223 (8614) Type: qualityOfServiceAlarm Package: lte.IK4007223 Raised on class: lte.M3MmeAccess	Severity: major Specific problem: MME M3 SETUP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that all attempts initiated by MCE to set up the M3 AP with a peer MME have failed. It can be due to a MME reject (oam intervention or unknown cause) or a timer expiration on MCE side because the MME has not answered on time or protocol issue in case of wrong ASN.1 decoding or unexpected message received.		
Remedial action: Correct the issue on the MME; when the issue is solved, lock then unlock the M3MmeAccess.		

Table 29-632 IK4007224

Alarm	Attributes	Applicable major release
Name: IK4007224 (8615) Type: qualityOfServiceAlarm Package: lte.IK4007224 Raised on class: lte.M3MmeAccess	Severity: major Specific problem: MME M3 RESET ALL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that all attempts to perform the MCE initiated M3 Reset/All have failed due to no response of the MME.		
Remedial action: Correct the issue on the MME; when the issue is solved, lock then unlock the M3MmeAccess.		

Table 29-633 IK4007225

Alarm	Attributes	Applicable major release
Name: IK4007225 (8616) Type: processingErrorAlarm Package: lte.IK4007225 Raised on class: lte.Mce	Severity: indeterminate Specific problem: M3AP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: For the session identified by tmgi, the MCE has detected inconsistent or unsupported value of M3AP session parameters.		
Remedial action: No action is required.		

Table 29-634 IK4007228

Alarm	Attributes	Applicable major release
Name: IK4007228 (8617) Type: processingErrorAlarm Package: lte.IK4007228 Raised on class: lte.Cell	Severity: minor Specific problem: CELL FAULT 4 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Cell fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-635 IK4007229

Alarm	Attributes	Applicable major release
Name: IK4007229 (8618) Type: processingErrorAlarm Package: lte.IK4007229 Raised on class: lte.Cell	Severity: minor Specific problem: CELL FAULT 5 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Cell fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-636 IK4007230

Alarm	Attributes	Applicable major release
Name: IK4007230 (8619) Type: processingErrorAlarm Package: lte.IK4007230 Raised on class: lte.Cell	Severity: major Specific problem: CELL FAULT 6 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Cell fault.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-637 IK4007231

Alarm	Attributes	Applicable major release
Name: IK4007231 (8620) Type: processingErrorAlarm Package: lte.IK4007231 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in.		

Table 29-637 IK4007231 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-638 IK4007232

Alarm	Attributes	Applicable major release
Name: IK4007232 (8621) Type: processingErrorAlarm Package: lte.IK4007232 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-639 IK4007233

Alarm	Attributes	Applicable major release
Name: IK4007233 (8622) Type: qualityOfServiceAlarm Package: lte.IK4007233 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MME M3 RESET/ALL OAM INTERVENTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: M3AP Reset/All with cause -OAM intervention- received from MME over M3 interface		
Remedial action: No action is required.		

Table 29-640 IK4007234

Alarm	Attributes	Applicable major release
Name: IK4007234 (8623) Type: qualityOfServiceAlarm Package: lte.IK4007234 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MBMS SAI CONFIGURATION ISSUE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event may indicate that several MbsfnAreas are configured with the same SAI(s) and that these SAI(s) relate to Location Dependent Content MBMS User Service(s). This event may also indicate that MbsfnArea(s) configured with SAI(s) related to Location Dependent Content MBMS User Service(s),are served by the same cell(s).		
Remedial action: No action is required.		

Table 29-641 IK4007235

Alarm	Attributes	Applicable major release
Name: IK4007235 (8624) Type: processingErrorAlarm Package: lte.IK4007235 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB CP FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-642 IK4007236

Alarm	Attributes	Applicable major release
Name: IK4007236 (8625) Type: processingErrorAlarm Package: lte.IK4007236 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB CP FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-643 IK4007237

Alarm	Attributes	Applicable major release
Name: IK4007237 (8626) Type: processingErrorAlarm Package: lte.IK4007237 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB CP FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-644 IK4007238

Alarm	Attributes	Applicable major release
Name: IK4007238 (8627) Type: processingErrorAlarm Package: lte.IK4007238 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB CP EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-644 IK4007238 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in.\nUnspecified CB event detected		
Remedial action: No action is required.		

Table 29-645 IK4007239

Alarm	Attributes	Applicable major release
Name: IK4007239 (8628) Type: processingErrorAlarm Package: lte.IK4007239 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB CP EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified CB event detected		
Remedial action: No action is required.		

Table 29-646 IK4007240

Alarm	Attributes	Applicable major release
Name: IK4007240 (8629) Type: processingErrorAlarm Package: lte.IK4007240 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB CP EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified CB event detected		
Remedial action: No action is required.		

Table 29-647 IK4007241

Alarm	Attributes	Applicable major release
Name: IK4007241 (8630) Type: qualityOfServiceAlarm Package: lte.IK4007241 Raised on class: lte.M3MmeAccess	Severity: major Specific problem: MME M3 FAULT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-648 IK4007242

Alarm	Attributes	Applicable major release
Name: IK4007242 (8631) Type: communicationsAlarm Package: lte.IK4007242 Raised on class: lte.RncAccess	Severity: minor Specific problem: RNC ACCESS FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RNC ACCESS fault detected		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-649 IK4007243

Alarm	Attributes	Applicable major release
Name: IK4007243 (8632) Type: communicationsAlarm Package: lte.IK4007243 Raised on class: lte.RncAccess	Severity: minor Specific problem: RNC ACCESS FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RNC ACCESS fault detected		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-650 IK4007244

Alarm	Attributes	Applicable major release
Name: IK4007244 (8633) Type: communicationsAlarm Package: lte.IK4007244 Raised on class: lte.RncAccess	Severity: major Specific problem: RNC ACCESS FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RNC ACCESS fault detected		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-651 IK4007245

Alarm	Attributes	Applicable major release
Name: IK4007245 (8634) Type: communicationsAlarm Package: lte.IK4007245 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: RNC ACCESS EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-651 IK4007245 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified RNC ACCESS event detected		
Remedial action: No action is required.		

Table 29-652 IK4007246

Alarm	Attributes	Applicable major release
Name: IK4007246 (8635) Type: communicationsAlarm Package: lte.IK4007246 Raised on class: lte.RncAccess	Severity: indeterminate Specific problem: RNC ACCESS EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RNC ACCESS event detected		
Remedial action: No action is required.		

Table 29-653 IK4007247

Alarm	Attributes	Applicable major release
Name: IK4007247 (8636) Type: processingErrorAlarm Package: lte.IK4007247 Raised on class: lte.UtraFddNeighboringCellRelation	Severity: major Specific problem: UTRAN NEIGHBOR RELATION FAULT 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified UTRAN NEIGHBOR RELATION fault detected		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-654 IK4007248

Alarm	Attributes	Applicable major release
Name: IK4007248 (8637) Type: processingErrorAlarm Package: lte.IK4007248 Raised on class: lte.UtraFddNeighboringCellRelation	Severity: indeterminate Specific problem: UTRAN NEIGHBOR RELATION EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified UTRAN NEIGHBOR RELATION event detected		
Remedial action: No action is required.		

Table 29-655 IK4007249

Alarm	Attributes	Applicable major release
Name: IK4007249 (8638) Type: processingErrorAlarm Package: lte.IK4007249 Raised on class: lte.UtraFddNeighboringFreqConf	Severity: indeterminate Specific problem: UTRAN FDD NEIGHBOR FREQ CONF EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified UTRAN FDD NEIGHBOR FREQ CONF event detected		
Remedial action: No action is required.		

Table 29-656 IK4007250

Alarm	Attributes	Applicable major release
Name: IK4007250 (8639) Type: processingErrorAlarm Package: lte.IK4007250 Raised on class: lte.Cell	Severity: indeterminate Specific problem: UTRAN NEIGHBOR RELATION REPLACEMENT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a UTRAN Neighbor Relation has been replaced with a new higher priority neighbor.		
Remedial action: No action is required.		

Table 29-657 IK4007254

Alarm	Attributes	Applicable major release
Name: IK4007254 (8640) Type: processingErrorAlarm Package: lte.IK4007254 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: critical Specific problem: DELAY CONFIG FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Configured cell path delays are no longer correct and the modem function must be reset to adopt the new values.		
Remedial action: Reset the modem.		

Table 29-658 IK4007255

Alarm	Attributes	Applicable major release
Name: IK4007255 (8641) Type: communicationsAlarm Package: lte.IK4007255 Raised on class: lte.Rco2Access	Severity: major Specific problem: CS-VNF SETUP FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent CS_VNF_SETUP_FAILURE from CS-VNF detected by CallpMgr.		
Remedial action: Check the behavior of the CS-VNF.		

Table 29-659 IK4007256

Alarm	Attributes	Applicable major release
Name: IK4007256 (8642) Type: communicationsAlarm Package: lte.IK4007256 Raised on class: lte.Rco2Access	Severity: major Specific problem: CS-VNF SETUP NO RESPONSE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a persistent NO_RESPONSE from CS-VNF detected by CallpMgr.		
Remedial action: Check the behavior of the CS-VNF.		

Table 29-660 IK4007259

Alarm	Attributes	Applicable major release
Name: IK4007259 (8643) Type: qualityOfServiceAlarm Package: lte.IK4007259 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: CS APPLICATION DOWN Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that CS application is down and the eNB will fall back to non-CS scheduling mode		
Remedial action: No action is required.		

Table 29-661 IK4007260

Alarm	Attributes	Applicable major release
Name: IK4007260 (8644) Type: processingErrorAlarm Package: lte.IK4007260 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: CELL CLEAN UP FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a cell deletion failure when cell clean-up is triggered by LteCell instance deletion online, parameter update or when software failure happens		
Remedial action: Lock then unlock the BB.		

Table 29-662 IK4007261

Alarm	Attributes	Applicable major release
Name: IK4007261 (8645) Type: processingErrorAlarm Package: lte.IK4007261 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BRC UC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the BRC-UC reported a warning.		
Remedial action: No action is required.		

Table 29-663 IK4007262

Alarm	Attributes	Applicable major release
Name: IK4007262 (8646) Type: processingErrorAlarm Package: lte.IK4007262 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BRC UC FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the UeCallIP detected a no-response from BRC-UC.		
Remedial action: No action is required.		

Table 29-664 IK4007263

Alarm	Attributes	Applicable major release
Name: IK4007263 (8647) Type: communicationsAlarm Package: lte.IK4007263 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: CS-VNF CONFIGURATION UPDATE FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent CS_VNF_CONFIGURATION_UPDATE _FAILURE message from CS-VNF network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-665 IK4007264

Alarm	Attributes	Applicable major release
Name: IK4007264 (8648) Type: communicationsAlarm Package: lte.IK4007264 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: CS-VNF CONFIGURATION UPDATE NO RESPONSE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a persistent NO_RESPONSE from CS-VNF network element detected by CallpMgr.		
Remedial action: No action is required.		

Table 29-666 IK4007265

Alarm	Attributes	Applicable major release
Name: IK4007265 (8649) Type: processingErrorAlarm Package: lte.IK4007265 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB MODEM FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-667 IK4007266

Alarm	Attributes	Applicable major release
Name: IK4007266 (8650) Type: processingErrorAlarm Package: lte.IK4007266 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB MODEM FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-667 IK4007266 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-668 IK4007267

Alarm	Attributes	Applicable major release
Name: IK4007267 (8651) Type: processingErrorAlarm Package: lte.IK4007267 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB MODEM FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-669 IK4007268

Alarm	Attributes	Applicable major release
Name: IK4007268 (8652) Type: processingErrorAlarm Package: lte.IK4007268 Raised on class: lte.X2Access	Severity: major Specific problem: X2IP ADDR RETRIEVAL FAILURE Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the X2 IP address retrieval failure. When this alarm is raised, X2TransportLayerAccess is {Disabled, Failed} (and X2Access {Disabled, dependency}).		
Remedial action: Set the IP address manually.		

Table 29-670 IK4007269

Alarm	Attributes	Applicable major release
Name: IK4007269 (8653) Type: processingErrorAlarm Package: lte.IK4007269 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BRC CC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the BRC-CC reported a warning.		

Table 29-670 IK4007269 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-671 IK4007270

Alarm	Attributes	Applicable major release
Name: IK4007270 (8654) Type: processingErrorAlarm Package: lte.IK4007270 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BRC UC FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the UeCallIP detected a no-response from BRC-UC.		
Remedial action: No action is required.		

Table 29-672 IK4007271

Alarm	Attributes	Applicable major release
Name: IK4007271 (8655) Type: processingErrorAlarm Package: lte.IK4007271 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BRC UC WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BRC-UC reported a warning.		
Remedial action: No action is required.		

Table 29-673 IK4007272

Alarm	Attributes	Applicable major release
Name: IK4007272 (8656) Type: processingErrorAlarm Package: lte.IK4007272 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CALLP MANAGER WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that CallP Manager reports a warning.		
Remedial action: No action is required.		

Table 29-674 IK4007273

Alarm	Attributes	Applicable major release
Name: IK4007273 (8657) Type: processingErrorAlarm Package: lte.IK4007273 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: L1L2 CONFIG REFUSED CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates the cell deletion for logical cell resetting procedure is rejected by the modem entity on CB		
Remedial action: Reset eNB.		

Table 29-675 IK4007274

Alarm	Attributes	Applicable major release
Name: IK4007274 (8658) Type: processingErrorAlarm Package: lte.IK4007274 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: L1L2 CONFIG TIMEOUT CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a non-response from Modem Entity on CB for cell deletion in the logical cell resetting procedure.		
Remedial action: Reset eNB		

Table 29-676 IK4007275

Alarm	Attributes	Applicable major release
Name: IK4007275 (8659) Type: processingErrorAlarm Package: lte.IK4007275 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CELL CLEAN UP FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a cell deletion failure when cell clean-up is triggered by LteCell instance deletion online, parameter update or when software failure happens		
Remedial action: Reset eNB		

Table 29-677 IK4007276

Alarm	Attributes	Applicable major release
Name: IK4007276 (8660) Type: processingErrorAlarm Package: lte.IK4007276 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB DELAY CONFIG FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates a modification of delays requiring CB to be reset so to use new values.		
Remedial action: Reset eNB.		

Table 29-678 IK4007277

Alarm	Attributes	Applicable major release
Name: IK4007277 (8661) Type: processingErrorAlarm Package: lte.IK4007277 Raised on classes: • lte.CBCardSpecifics • lte.ENBEquipment	Severity: indeterminate Specific problem: CALLP MANAGER WARNING Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that CallP Manager reports a warning.		
Remedial action: No action is required.		

Table 29-679 IK4007278

Alarm	Attributes	Applicable major release
Name: IK4007278 (8662) Type: processingErrorAlarm Package: lte.IK4007278 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: L1L2 CONFIG REFUSED CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the cell deletion for logical cell resetting procedure is rejected by the modem entity on CB		
Remedial action: Reset eNB.		

Table 29-680 IK4007279

Alarm	Attributes	Applicable major release
Name: IK4007279 (8663) Type: processingErrorAlarm Package: lte.IK4007279 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: major Specific problem: L1L2 CONFIG TIMEOUT CELL DELETE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a non-response from Modem Entity on CB for cell deletion in the logical cell resetting procedure.		
Remedial action: Reset eNB		

Table 29-681 IK4007280

Alarm	Attributes	Applicable major release
Name: IK4007280 (10057) Type: processingErrorAlarm Package: lte.IK4007280 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB EVENT HRAL 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.\nUnspecified BB event detected		
Remedial action: No action is required.		

Table 29-682 IK4007281

Alarm	Attributes	Applicable major release
Name: IK4007281 (10058) Type: processingErrorAlarm Package: lte.IK4007281 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB CP EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB event detected		
Remedial action: No action is required.		

Table 29-683 IK4007282

Alarm	Attributes	Applicable major release
Name: IK4007282 (10059) Type: processingErrorAlarm Package: lte.IK4007282 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB CP FAULT 4 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-684 IK4007284

Alarm	Attributes	Applicable major release
Name: IK4007284 (10061) Type: qualityOfServiceAlarm Package: lte.IK4007284 Raised on class: lte.M3MmeAccess	Severity: minor Specific problem: MME M3 FAULT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-685 IK4007285

Alarm	Attributes	Applicable major release
Name: IK4007285 (10062) Type: qualityOfServiceAlarm Package: lte.IK4007285 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE event detected.		
Remedial action: No action is required.		

Table 29-686 IK4007286

Alarm	Attributes	Applicable major release
Name: IK4007286 (10063) Type: processingErrorAlarm Package: lte.IK4007286 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE event detected.		
Remedial action: No action is required.		

Table 29-687 IK4007287

Alarm	Attributes	Applicable major release
Name: IK4007287 (10064) Type: processingErrorAlarm Package: lte.IK4007287 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE event detected.		
Remedial action: No action is required.		

Table 29-688 IK4007288

Alarm	Attributes	Applicable major release
Name: IK4007288 (10065) Type: integrityViolation Package: lte.IK4007288 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE event detected.		
Remedial action: No action is required.		

Table 29-689 IK4007289

Alarm	Attributes	Applicable major release
Name: IK4007289 (10066) Type: qualityOfServiceAlarm Package: lte.IK4007289 Raised on class: lte.Mce	Severity: major Specific problem: MCE FAULT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-690 IK4007290

Alarm	Attributes	Applicable major release
Name: IK4007290 (10067) Type: qualityOfServiceAlarm Package: lte.IK4007290 Raised on class: lte.Mce	Severity: major Specific problem: MCE FAULT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-691 IK4007291

Alarm	Attributes	Applicable major release
Name: IK4007291 (10068) Type: qualityOfServiceAlarm Package: lte.IK4007291 Raised on class: lte.Mce	Severity: minor Specific problem: MCE FAULT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MCE fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-692 IK4007292

Alarm	Attributes	Applicable major release
Name: IK4007292 (10069) Type: processingErrorAlarm Package: lte.IK4007292 Raised on class: lte.M3MmeAccess	Severity: indeterminate Specific problem: M3AP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: For the session identified by tmgi, the MCE has detected inconsistent or unsupported value of M3AP session parameters.		
Remedial action: No action is required.		

Table 29-693 IK4007293

Alarm	Attributes	Applicable major release
Name: IK4007293 (10070) Type: qualityOfServiceAlarm Package: lte.IK4007293 Raised on class: lte.M3MmeAccess	Severity: indeterminate Specific problem: MME M3 RESET/ALL OAM INTERVENTION Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: M3AP Reset/All with cause -OAM intervention- received from MME over M3 interface		
Remedial action: No action is required.		

Table 29-694 IK4007294

Alarm	Attributes	Applicable major release
Name: IK4007294 (10071) Type: communicationsAlarm Package: lte.IK4007294 Raised on class: lte.Rco2Access	Severity: major Specific problem: RCO2 FAULT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-695 IK4007295

Alarm	Attributes	Applicable major release
Name: IK4007295 (10072) Type: communicationsAlarm Package: lte.IK4007295 Raised on class: lte.Rco2Access	Severity: minor Specific problem: RCO2 FAULT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-696 IK4007296

Alarm	Attributes	Applicable major release
Name: IK4007296 (10073) Type: communicationsAlarm Package: lte.IK4007296 Raised on class: lte.Rco2Access	Severity: minor Specific problem: RCO2 FAULT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-697 IK4007297

Alarm	Attributes	Applicable major release
Name: IK4007297 (10074) Type: communicationsAlarm Package: lte.IK4007297 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: RCO2 EVENT 1 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: None.		

Table 29-698 IK4007298

Alarm	Attributes	Applicable major release
Name: IK4007298 (10075) Type: qualityOfServiceAlarm Package: lte.IK4007298 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: RCO2 EVENT 2 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: None.		

Table 29-699 IK4007299

Alarm	Attributes	Applicable major release
Name: IK4007299 (10076) Type: communicationsAlarm Package: lte.IK4007299 Raised on class: lte.Rco2Access	Severity: indeterminate Specific problem: RCO2 EVENT 3 Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: None.		

Table 29-700 IK4007300

Alarm	Attributes	Applicable major release
Name: IK4007300 (10077) Type: equipmentAlarm Package: lte.IK4007300 Raised on class: lte.Rco2TransportLayerAccess	Severity: major Specific problem: RCO2 TRANS FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-701 IK4007301

Alarm	Attributes	Applicable major release
Name: IK4007301 (10078) Type: equipmentAlarm Package: lte.IK4007301 Raised on class: lte.Rco2TransportLayerAccess	Severity: indeterminate Specific problem: RCO2 TRANS EVENT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified Modem Function fault detected		
Remedial action: None.		

Table 29-702 IK4007302

Alarm	Attributes	Applicable major release
Name: IK4007302 (10079) Type: operationalViolation Package: lte.IK4007302 Raised on class: lte.Cell	Severity: major Specific problem: RSI REALLOCATION FAILED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that an RSI conflict has been detected between the cell and one or more of its neighboring cells or the current RSI is not valid and the eNB is not able to reallocate a valid and conflict-free RSI to the cell.		

Table 29-702 IK4007302 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Enlarge the RSI allowed range, either for local or the distant cells.		

Table 29-703 IK4007303

Alarm	Attributes	Applicable major release
Name: IK4007303 (10080) Type: processingErrorAlarm Package: lte.IK4007303 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: RAN PCMD ACTIVATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates the failure to activate a new RAN PCMD trace recording session.		
Remedial action: No action is required.		

Table 29-704 IK4007304

Alarm	Attributes	Applicable major release
Name: IK4007304 (10081) Type: processingErrorAlarm Package: lte.IK4007304 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: RAN PCMD INVALID PARAMETER Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates the parameter received for RAN PCMD is invalid.		
Remedial action: No action is required.		

Table 29-705 IK4007317

Alarm	Attributes	Applicable major release
Name: IK4007317 (10082) Type: processingErrorAlarm Package: lte.IK4007317 Raised on class: lte.Cell	Severity: indeterminate Specific problem: ENB BLACKLIST OF NEIGHBOR RELATION Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that a Neighbor Relation has been Blacklisted by the eNB.		
Remedial action: No action is required.		

Table 29-706 IK4007318

Alarm	Attributes	Applicable major release
Name: IK4007318 (11008) Type: processingErrorAlarm Package: lte.IK4007318 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 7 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-707 IK4007319

Alarm	Attributes	Applicable major release
Name: IK4007319 (11009) Type: processingErrorAlarm Package: lte.IK4007319 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 8 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-708 IK4007320

Alarm	Attributes	Applicable major release
Name: IK4007320 (11010) Type: processingErrorAlarm Package: lte.IK4007320 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB EVENT 9 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-709 IK4007321

Alarm	Attributes	Applicable major release
Name: IK4007321 (11011) Type: qualityOfServiceAlarm Package: lte.IK4007321 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE CAC FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Description1: MCE admission reaches the max nbr of sessions in MBSFN Area;\n\nDescription2: MCE admission reaches the max nbr of available sub-frames in MBSFN Area;\n\nDescription3: The needed MBSFN resources exceed the allowed limit;		
Remedial action: No action is required.		

Table 29-710 IK4007322

Alarm	Attributes	Applicable major release
Name: IK4007322 (11012) Type: qualityOfServiceAlarm Package: lte.IK4007322 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MBSFN ACTIVATION DENIED Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the access to an MBSFN area has been denied either because of operator manual lock or MCE automatic lock due to offending MBSFN area.		
Remedial action: No action is required.		

Table 29-711 IK4007323

Alarm	Attributes	Applicable major release
Name: IK4007323 (11013) Type: qualityOfServiceAlarm Package: lte.IK4007323 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE SESSION RESUMED Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that one or several sessions previously in SUSPENDED state have been resumed (for the considered MbsfnArea).		
Remedial action: No action is required.		

Table 29-712 IK4007324

Alarm	Attributes	Applicable major release
Name: IK4007324 (11014) Type: operationalViolation Package: lte.IK4007324 Raised on class: lte.Cell	Severity: minor Specific problem: RSI CONFLICT OR INVALIDITY DETECTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that an RSI conflict has been detected between the cell and one or more of its neighboring cells or the current RSI is not valid.		
Remedial action: Modify the parameter rootSequenceIndex according to the proposed RSI value in the alarm or enable RSI Auto Modification in the concerned cell so that RSI optimization function can correct automatically the RSI conflict/invalidity according to the configured maintenance period. In case of RSI invalidity, check the configured RSI range.		

Table 29-713 IK4007325

Alarm	Attributes	Applicable major release
Name: IK4007325 (11015) Type: processingErrorAlarm Package: lte.IK4007325 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SIGNALING TRACE STOP Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the signaling based trace session is stopped when eNodeB received a ERP trace session activation request.		
Remedial action: No action is required.		

Table 29-714 IK4009001

Alarm	Attributes	Applicable major release
Name: IK4009001 (2616) Type: equipmentAlarm Package: lte.IK4009001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-715 IK4009002

Alarm	Attributes	Applicable major release
Name: IK4009002 (2617) Type: equipmentAlarm Package: lte.IK4009002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-716 IK4009003

Alarm	Attributes	Applicable major release
Name: IK4009003 (2618) Type: equipmentAlarm Package: lte.IK4009003 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-717 IK4009006

Alarm	Attributes	Applicable major release
Name: IK4009006 (2621) Type: processingErrorAlarm Package: lte.IK4009006 Raised on class: lte.MODULE	Severity: major Specific problem: DHCP FAILURE TO OBTAIN PTP IP ADDRESS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB has failed to receive PTP IP addresses: End Point and PTP server IP addresses (not only End point IP address)		
Remedial action: Check and correct its DHCP configuration for 1588 IP addresses. When the alarm is raised it means that eNodeB has not received an answer from DHCP to its 1588 DHCP request.		

Table 29-718 IK4009007

Alarm	Attributes	Applicable major release
Name: IK4009007 (2622) Type: securityServiceOrMechanismViolation Package: lte.IK4009007 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: HIGH PACKET DROPPING RATE Implicitly cleared: true Default probable cause: floodDetected	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the policer controlling the local ingress traffic of the eNB is dropping packets on some flows with an abnormal rate.		
Remedial action: Unknown.		

Table 29-719 IK4009008

Alarm	Attributes	Applicable major release
Name: IK4009008 (5232) Type: equipmentAlarm Package: lte.IK4009008 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: LAST S1 SCTP ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the MME does not acknowledge the S1 association request from the eNodeB.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME.		

Table 29-720 IK4009009

Alarm	Attributes	Applicable major release
Name: IK4009009 (5233) Type: equipmentAlarm Package: lte.IK4009009 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: LAST S1 SCTP ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the last S1 association fault between eNodeB and MME.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME.		

Table 29-721 IK4009012

Alarm	Attributes	Applicable major release
Name: IK4009012 (2625) Type: equipmentAlarm Package: lte.IK4009012 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-722 IK4009013

Alarm	Attributes	Applicable major release
Name: IK4009013 (5234) Type: processingErrorAlarm Package: lte.IK4009013 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MF EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MF fault detected.		
Remedial action: No action is required.		

Table 29-723 IK4009014

Alarm	Attributes	Applicable major release
Name: IK4009014 (5235) Type: processingErrorAlarm Package: lte.IK4009014 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MF EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MF fault detected.		

Table 29-723 IK4009014 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-724 IK4009017

Alarm	Attributes	Applicable major release
Name: IK4009017 (5236) Type: processingErrorAlarm Package: lte.IK4009017 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MF EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified MF fault detected.		
Remedial action: No action is required.		

Table 29-725 IK4009020

Alarm	Attributes	Applicable major release
Name: IK4009020 (2630) Type: equipmentAlarm Package: lte.IK4009020 Raised on class: lte.X2TransportLayerAccess	Severity: major Specific problem: X2 SCTP ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the neighboring eNodeB does not acknowledge the X2 association requests from the eNodeB.		
Remedial action: Reset the eNodeB.		

Table 29-726 IK4009022

Alarm	Attributes	Applicable major release
Name: IK4009022 (2632) Type: equipmentAlarm Package: lte.IK4009022 Raised on class: lte.X2TransportLayerAccess	Severity: major Specific problem: X2 SCTP ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a fault in the X2 association between the eNodeBs.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and peer eNB. 2. Check network connectivity between eNB and peer eNB.		

Table 29-727 IK4009024

Alarm	Attributes	Applicable major release
Name: IK4009024 (2634) Type: equipmentAlarm Package: lte.IK4009024 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: OAM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the OAM interface.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-728 IK4009025

Alarm	Attributes	Applicable major release
Name: IK4009025 (2635) Type: equipmentAlarm Package: lte.IK4009025 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: TELECOM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the telecom interface. One of these interface might be impacted:(S1-U/C, X2-U/C). The additional information for this alarm should included the traffic type impacted and the IP address.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-729 IK4009026

Alarm	Attributes	Applicable major release
Name: IK4009026 (2636) Type: equipmentAlarm Package: lte.IK4009026 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: SSH SERVER START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to start the SSH server.		
Remedial action: Reset the eNodeB.		

Table 29-730 IK4009027

Alarm	Attributes	Applicable major release
Name: IK4009027 (2637) Type: equipmentAlarm Package: lte.IK4009027 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: SSH SERVER STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-730 IK4009027 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates the failure to stop the SSH server.		
Remedial action: No action is required.		

Table 29-731 IK4009028

Alarm	Attributes	Applicable major release
Name: IK4009028 (2638) Type: equipmentAlarm Package: lte.IK4009028 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: SNTP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to start the SNTP client.		
Remedial action: Check the network connectivity of NTP server and NTP server address provisioning. If the NTP server is unreachable or the provisioning is incorrect, address those aspects. If all other possible causes have been eliminated, reset the eNB.		

Table 29-732 IK4009029

Alarm	Attributes	Applicable major release
Name: IK4009029 (2639) Type: equipmentAlarm Package: lte.IK4009029 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: SNTP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to stop the SNTP client.		
Remedial action: No action is required.		

Table 29-733 IK4009030

Alarm	Attributes	Applicable major release
Name: IK4009030 (5237) Type: equipmentAlarm Package: lte.IK4009030 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: WALG INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize the WAL gateway.		
Remedial action: Reset the eNodeB.		

Table 29-734 IK4009032

Alarm	Attributes	Applicable major release
Name: IK4009032 (2640) Type: equipmentAlarm Package: lte.IK4009032 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: DHCP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to start the DHCP client on the eNodeB network interface.		
Remedial action: Reset the eNodeB.		

Table 29-735 IK4009033

Alarm	Attributes	Applicable major release
Name: IK4009033 (2641) Type: equipmentAlarm Package: lte.IK4009033 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: DHCP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to stop the DHCP client on the eNodeB network interface.		
Remedial action: No action is required.		

Table 29-736 IK4009034

Alarm	Attributes	Applicable major release
Name: IK4009034 (2642) Type: processingErrorAlarm Package: lte.IK4009034 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: UNEXPECTED DATA FROM DHCP SERVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the lease time offered by the DHCP server is different from the lease time requested by the DHCP client.		
Remedial action: Configure the DHCP server with an infinite lease time.		

Table 29-737 IK4009036

Alarm	Attributes	Applicable major release
Name: IK4009036 (2644) Type: communicationsAlarm Package: lte.IK4009036 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: ETHERNET TRANSPORT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an interface error due to the counters exceeding the configured threshold.		

Table 29-737 IK4009036 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the network status and cabling if possible. If the alarm persists, contact the next level support.		

Table 29-738 IK4009041

Alarm	Attributes	Applicable major release
Name: IK4009041 (2648) Type: equipmentAlarm Package: lte.IK4009041 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check the board connectivity.		

Table 29-739 IK4009042

Alarm	Attributes	Applicable major release
Name: IK4009042 (2649) Type: communicationsAlarm Package: lte.IK4009042 Raised on class: lte.MmeAccess	Severity: major Specific problem: NO RESPONSE TO ECHO REQUEST ON S1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a S1 fault due to the GTP Echo request.		
Remedial action: Check for connectivity and verify the GTP provisioning.		

Table 29-740 IK4009044

Alarm	Attributes	Applicable major release
Name: IK4009044 (2650) Type: equipmentAlarm Package: lte.IK4009044 Raised on class: lte.MmeTransportLayerAccess	Severity: major Specific problem: S1 SCTP ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the MME does not acknowledge the S1 association request from the eNodeB.		
Remedial action: 1.Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME.		

Table 29-741 IK4009046

Alarm	Attributes	Applicable major release
Name: IK4009046 (2651) Type: equipmentAlarm Package: lte.IK4009046 Raised on class: lte.MmeTransportLayerAccess	Severity: major Specific problem: S1 SCTP ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a S1 association fault between eNodeB and MME.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME.		

Table 29-742 IK4009048

Alarm	Attributes	Applicable major release
Name: IK4009048 (2652) Type: equipmentAlarm Package: lte.IK4009048 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: DHCP LEASE LOST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the DHCP client lost the lease of the DHCP server.		
Remedial action: No action is required.		

Table 29-743 IK4009049

Alarm	Attributes	Applicable major release
Name: IK4009049 (2653) Type: equipmentAlarm Package: lte.IK4009049 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: DHCP CLIENT LEASE FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the DHCP client to obtain the lease from the DHCP server.		
Remedial action: Check for connectivity. Check for DHCP server and network configurations.		

Table 29-744 IK4009050

Alarm	Attributes	Applicable major release
Name: IK4009050 (2654) Type: equipmentAlarm Package: lte.IK4009050 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: IP LOOPBACK ACTIVE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the IP loopback is activated.		
Remedial action: Call the next level of support.		

Table 29-745 IK4009051

Alarm	Attributes	Applicable major release
Name: IK4009051 (2655) Type: equipmentAlarm Package: lte.IK4009051 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: IP LOOPBACK MANUAL TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback is manually stopped.		
Remedial action: No action is required.		

Table 29-746 IK4009052

Alarm	Attributes	Applicable major release
Name: IK4009052 (2656) Type: equipmentAlarm Package: lte.IK4009052 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: IP LOOPBACK INACTIVITY PERIOD TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback stopped automatically due to inactivity for certain period.		
Remedial action: No action is required.		

Table 29-747 IK4009053

Alarm	Attributes	Applicable major release
Name: IK4009053 (2657) Type: equipmentAlarm Package: lte.IK4009053 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: IP LOOPBACK GUARD TIMER TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback stopped automatically due to expiry of the guard timer.		
Remedial action: No action is required.		

Table 29-748 IK4009054

Alarm	Attributes	Applicable major release
Name: IK4009054 (2658) Type: equipmentAlarm Package: lte.IK4009054 Raised on class: lte.AMR	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-748 IK4009054 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-749 IK4009055

Alarm	Attributes	Applicable major release
Name: IK4009055 (2659) Type: equipmentAlarm Package: lte.IK4009055 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-750 IK4009056

Alarm	Attributes	Applicable major release
Name: IK4009056 (2660) Type: equipmentAlarm Package: lte.IK4009056 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-751 IK4009057

Alarm	Attributes	Applicable major release
Name: IK4009057 (2661) Type: equipmentAlarm Package: lte.IK4009057 Raised on class: lte.AMR	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check for connectivity with the board.		

Table 29-752 IK4009058

Alarm	Attributes	Applicable major release
Name: IK4009058 (2662) Type: equipmentAlarm Package: lte.IK4009058 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check for connectivity with the board.		

Table 29-753 IK4009059

Alarm	Attributes	Applicable major release
Name: IK4009059 (2663) Type: equipmentAlarm Package: lte.IK4009059 Raised on class: lte.RetAldEntry	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check for connectivity with the board.		

Table 29-754 IK4009060

Alarm	Attributes	Applicable major release
Name: IK4009060 (3118) Type: equipmentAlarm Package: lte.IK4009060 Raised on class: lte.AMR	Severity: minor Specific problem: OAM AMR FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-755 IK4009061

Alarm	Attributes	Applicable major release
Name: IK4009061 (3119) Type: equipmentAlarm Package: lte.IK4009061 Raised on class: lte.AMR	Severity: minor Specific problem: OAM AMR FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		

Table 29-755 IK4009061 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Call the next level of support.		

Table 29-756 IK4009062

Alarm	Attributes	Applicable major release
Name: IK4009062 (3120) Type: equipmentAlarm Package: lte.IK4009062 Raised on class: lte.AMR	Severity: minor Specific problem: OAM AMR FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-757 IK4009063

Alarm	Attributes	Applicable major release
Name: IK4009063 (3121) Type: equipmentAlarm Package: lte.IK4009063 Raised on class: lte.AMR	Severity: indeterminate Specific problem: OAM AMR EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-758 IK4009064

Alarm	Attributes	Applicable major release
Name: IK4009064 (3122) Type: equipmentAlarm Package: lte.IK4009064 Raised on class: lte.AMR	Severity: indeterminate Specific problem: OAM AMR EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-759 IK4009065

Alarm	Attributes	Applicable major release
Name: IK4009065 (3123) Type: equipmentAlarm Package: lte.IK4009065 Raised on class: lte.AMR	Severity: indeterminate Specific problem: OAM AMR EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-760 IK4009066

Alarm	Attributes	Applicable major release
Name: IK4009066 (3124) Type: equipmentAlarm Package: lte.IK4009066 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: OAM BB FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-761 IK4009067

Alarm	Attributes	Applicable major release
Name: IK4009067 (3125) Type: equipmentAlarm Package: lte.IK4009067 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: OAM BB FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-762 IK4009068

Alarm	Attributes	Applicable major release
Name: IK4009068 (3126) Type: equipmentAlarm Package: lte.IK4009068 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: OAM BB FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-762 IK4009068 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-763 IK4009070

Alarm	Attributes	Applicable major release
Name: IK4009070 (3128) Type: equipmentAlarm Package: lte.IK4009070 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: OAM BB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-764 IK4009071

Alarm	Attributes	Applicable major release
Name: IK4009071 (3129) Type: equipmentAlarm Package: lte.IK4009071 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: OAM BB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-765 IK4009076

Alarm	Attributes	Applicable major release
Name: IK4009076 (3134) Type: equipmentAlarm Package: lte.IK4009076 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-766 IK4009077

Alarm	Attributes	Applicable major release
Name: IK4009077 (3135) Type: equipmentAlarm Package: lte.IK4009077 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-767 IK4009078

Alarm	Attributes	Applicable major release
Name: IK4009078 (3136) Type: equipmentAlarm Package: lte.IK4009078 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: OAM DBU FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-768 IK4009079

Alarm	Attributes	Applicable major release
Name: IK4009079 (3137) Type: equipmentAlarm Package: lte.IK4009079 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: OAM DBU FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-769 IK4009080

Alarm	Attributes	Applicable major release
Name: IK4009080 (3138) Type: equipmentAlarm Package: lte.IK4009080 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: OAM DBU FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-769 IK4009080 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-770 IK4009081

Alarm	Attributes	Applicable major release
Name: IK4009081 (3139) Type: equipmentAlarm Package: lte.IK4009081 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: OAM DBU EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-771 IK4009082

Alarm	Attributes	Applicable major release
Name: IK4009082 (3140) Type: equipmentAlarm Package: lte.IK4009082 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: OAM DBU EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-772 IK4009083

Alarm	Attributes	Applicable major release
Name: IK4009083 (3141) Type: equipmentAlarm Package: lte.IK4009083 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: OAM DBU EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-773 IK4009090

Alarm	Attributes	Applicable major release
Name: IK4009090 (3148) Type: equipmentAlarm Package: lte.IK4009090 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: OAM TMA FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-774 IK4009091

Alarm	Attributes	Applicable major release
Name: IK4009091 (3149) Type: equipmentAlarm Package: lte.IK4009091 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: OAM TMA FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-775 IK4009092

Alarm	Attributes	Applicable major release
Name: IK4009092 (3150) Type: equipmentAlarm Package: lte.IK4009092 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: OAM TMA FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-776 IK4009093

Alarm	Attributes	Applicable major release
Name: IK4009093 (3151) Type: equipmentAlarm Package: lte.IK4009093 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: OAM TMA EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-776 IK4009093 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-777 IK4009094

Alarm	Attributes	Applicable major release
Name: IK4009094 (3152) Type: equipmentAlarm Package: lte.IK4009094 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: OAM TMA EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-778 IK4009095

Alarm	Attributes	Applicable major release
Name: IK4009095 (3153) Type: equipmentAlarm Package: lte.IK4009095 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: OAM TMA EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-779 IK4009096

Alarm	Attributes	Applicable major release
Name: IK4009096 (3154) Type: equipmentAlarm Package: lte.IK4009096 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: OAM RET FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-780 IK4009097

Alarm	Attributes	Applicable major release
Name: IK4009097 (3155) Type: equipmentAlarm Package: lte.IK4009097 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: OAM RET FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-781 IK4009098

Alarm	Attributes	Applicable major release
Name: IK4009098 (3156) Type: equipmentAlarm Package: lte.IK4009098 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: OAM RET FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-782 IK4009099

Alarm	Attributes	Applicable major release
Name: IK4009099 (3157) Type: equipmentAlarm Package: lte.IK4009099 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: OAM RET EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-783 IK4009100

Alarm	Attributes	Applicable major release
Name: IK4009100 (3158) Type: equipmentAlarm Package: lte.IK4009100 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: OAM RET EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-783 IK4009100 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-784 IK4009101

Alarm	Attributes	Applicable major release
Name: IK4009101 (3159) Type: equipmentAlarm Package: lte.IK4009101 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: OAM RET EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-785 IK4009102

Alarm	Attributes	Applicable major release
Name: IK4009102 (3160) Type: equipmentAlarm Package: lte.IK4009102 Raised on class: lte.MmeAccess	Severity: minor Specific problem: OAM S1 FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-786 IK4009103

Alarm	Attributes	Applicable major release
Name: IK4009103 (3161) Type: equipmentAlarm Package: lte.IK4009103 Raised on class: lte.MmeAccess	Severity: minor Specific problem: OAM S1 FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-787 IK4009104

Alarm	Attributes	Applicable major release
Name: IK4009104 (3162) Type: equipmentAlarm Package: lte.IK4009104 Raised on class: lte.MmeAccess	Severity: minor Specific problem: OAM S1 FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-788 IK4009105

Alarm	Attributes	Applicable major release
Name: IK4009105 (3163) Type: equipmentAlarm Package: lte.IK4009105 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: OAM S1 EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-789 IK4009106

Alarm	Attributes	Applicable major release
Name: IK4009106 (3164) Type: equipmentAlarm Package: lte.IK4009106 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: OAM S1 EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-790 IK4009107

Alarm	Attributes	Applicable major release
Name: IK4009107 (3165) Type: equipmentAlarm Package: lte.IK4009107 Raised on class: lte.MmeAccess	Severity: indeterminate Specific problem: OAM S1 EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-790 IK4009107 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-791 IK4009108

Alarm	Attributes	Applicable major release
Name: IK4009108 (3166) Type: equipmentAlarm Package: lte.IK4009108 Raised on class: lte.MmeTransportLayerAccess	Severity: minor Specific problem: OAM S1_TRANS FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-792 IK4009109

Alarm	Attributes	Applicable major release
Name: IK4009109 (3167) Type: equipmentAlarm Package: lte.IK4009109 Raised on class: lte.MmeTransportLayerAccess	Severity: minor Specific problem: OAM S1_TRANS FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-793 IK4009110

Alarm	Attributes	Applicable major release
Name: IK4009110 (3168) Type: equipmentAlarm Package: lte.IK4009110 Raised on class: lte.MmeTransportLayerAccess	Severity: minor Specific problem: OAM S1_TRANS FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-794 IK4009111

Alarm	Attributes	Applicable major release
Name: IK4009111 (3169) Type: equipmentAlarm Package: lte.IK4009111 Raised on class: lte.MmeTransportLayerAccess	Severity: indeterminate Specific problem: OAM S1_TRANS EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-795 IK4009112

Alarm	Attributes	Applicable major release
Name: IK4009112 (3170) Type: equipmentAlarm Package: lte.IK4009112 Raised on class: lte.MmeTransportLayerAccess	Severity: indeterminate Specific problem: OAM S1_TRANS EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-796 IK4009113

Alarm	Attributes	Applicable major release
Name: IK4009113 (3171) Type: equipmentAlarm Package: lte.IK4009113 Raised on class: lte.MmeTransportLayerAccess	Severity: indeterminate Specific problem: OAM S1_TRANS EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-797 IK4009114

Alarm	Attributes	Applicable major release
Name: IK4009114 (3172) Type: equipmentAlarm Package: lte.IK4009114 Raised on class: lte.X2Access	Severity: minor Specific problem: OAM X2 FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-797 IK4009114 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-798 IK4009115

Alarm	Attributes	Applicable major release
Name: IK4009115 (3173) Type: equipmentAlarm Package: lte.IK4009115 Raised on class: lte.X2Access	Severity: minor Specific problem: OAM X2 FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-799 IK4009116

Alarm	Attributes	Applicable major release
Name: IK4009116 (3174) Type: equipmentAlarm Package: lte.IK4009116 Raised on class: lte.X2Access	Severity: minor Specific problem: OAM X2 FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-800 IK4009117

Alarm	Attributes	Applicable major release
Name: IK4009117 (3175) Type: equipmentAlarm Package: lte.IK4009117 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: OAM X2 EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-801 IK4009118

Alarm	Attributes	Applicable major release
Name: IK4009118 (3176) Type: equipmentAlarm Package: lte.IK4009118 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: OAM X2 EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-802 IK4009119

Alarm	Attributes	Applicable major release
Name: IK4009119 (3177) Type: equipmentAlarm Package: lte.IK4009119 Raised on class: lte.X2Access	Severity: indeterminate Specific problem: OAM X2 EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-803 IK4009120

Alarm	Attributes	Applicable major release
Name: IK4009120 (3178) Type: equipmentAlarm Package: lte.IK4009120 Raised on class: lte.X2TransportLayerAccess	Severity: minor Specific problem: OAM X2_TRANS FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-804 IK4009121

Alarm	Attributes	Applicable major release
Name: IK4009121 (3179) Type: equipmentAlarm Package: lte.IK4009121 Raised on class: lte.X2TransportLayerAccess	Severity: minor Specific problem: OAM X2_TRANS FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-804 IK4009121 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-805 IK4009122

Alarm	Attributes	Applicable major release
Name: IK4009122 (3180) Type: equipmentAlarm Package: lte.IK4009122 Raised on class: lte.X2TransportLayerAccess	Severity: minor Specific problem: OAM X2_TRANS FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-806 IK4009123

Alarm	Attributes	Applicable major release
Name: IK4009123 (3181) Type: equipmentAlarm Package: lte.IK4009123 Raised on class: lte.X2TransportLayerAccess	Severity: indeterminate Specific problem: OAM X2_TRANS EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-807 IK4009124

Alarm	Attributes	Applicable major release
Name: IK4009124 (3182) Type: equipmentAlarm Package: lte.IK4009124 Raised on class: lte.X2TransportLayerAccess	Severity: indeterminate Specific problem: OAM X2_TRANS EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-808 IK4009125

Alarm	Attributes	Applicable major release
Name: IK4009125 (3183) Type: equipmentAlarm Package: lte.IK4009125 Raised on class: lte.X2TransportLayerAccess	Severity: indeterminate Specific problem: OAM X2_TRANS EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-809 IK4009129

Alarm	Attributes	Applicable major release
Name: IK4009129 (3187) Type: equipmentAlarm Package: lte.IK4009129 Raised on class: lte.RRH	Severity: indeterminate Specific problem: OAM RRH EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-810 IK4009130

Alarm	Attributes	Applicable major release
Name: IK4009130 (3188) Type: equipmentAlarm Package: lte.IK4009130 Raised on class: lte.RRH	Severity: indeterminate Specific problem: OAM RRH EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-811 IK4009131

Alarm	Attributes	Applicable major release
Name: IK4009131 (3189) Type: equipmentAlarm Package: lte.IK4009131 Raised on class: lte.RRH	Severity: indeterminate Specific problem: OAM RRH EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		

Table 29-811 IK4009131 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-812 IK4009134

Alarm	Attributes	Applicable major release
Name: IK4009134 (3192) Type: equipmentAlarm Package: lte.IK4009134 Raised on class: lte.TRDU	Severity: minor Specific problem: OAM TRDU FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-813 IK4009135

Alarm	Attributes	Applicable major release
Name: IK4009135 (3193) Type: equipmentAlarm Package: lte.IK4009135 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: OAM TRDU EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-814 IK4009136

Alarm	Attributes	Applicable major release
Name: IK4009136 (3194) Type: equipmentAlarm Package: lte.IK4009136 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: OAM TRDU EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-815 IK4009137

Alarm	Attributes	Applicable major release
Name: IK4009137 (3195) Type: equipmentAlarm Package: lte.IK4009137 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: OAM TRDU EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-816 IK4009138

Alarm	Attributes	Applicable major release
Name: IK4009138 (3196) Type: equipmentAlarm Package: lte.IK4009138 Raised on class: lte.RRH	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check connectivity between controller and RFM. Check operation of RFM and controller. If the alarm persists, contact the next level of support.		

Table 29-817 IK4009139

Alarm	Attributes	Applicable major release
Name: IK4009139 (3197) Type: equipmentAlarm Package: lte.IK4009139 Raised on class: lte.TRDU	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check connectivity between controller and TRDU. Check operation of TRDU and controller. If the alarm persists, contact the next level of support.		

Table 29-818 IK4009140

Alarm	Attributes	Applicable major release
Name: IK4009140 (3198) Type: equipmentAlarm Package: lte.IK4009140 Raised on class: lte.RRH	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		

Table 29-818 IK4009140 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-819 IK4009141

Alarm	Attributes	Applicable major release
Name: IK4009141 (3199) Type: equipmentAlarm Package: lte.IK4009141 Raised on class: lte.TRDU	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-820 IK4009142

Alarm	Attributes	Applicable major release
Name: IK4009142 (3200) Type: equipmentAlarm Package: lte.IK4009142 Raised on class: lte.RRH	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-821 IK4009143

Alarm	Attributes	Applicable major release
Name: IK4009143 (3201) Type: equipmentAlarm Package: lte.IK4009143 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-822 IK4009156

Alarm	Attributes	Applicable major release
Name: IK4009156 (3796) Type: equipmentAlarm Package: lte.IK4009156 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: SCTP INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to initialize the SCTP access.		
Remedial action: Reset the eNodeB.		

Table 29-823 IK4009162

Alarm	Attributes	Applicable major release
Name: IK4009162 (3802) Type: equipmentAlarm Package: lte.IK4009162 Raised on class: lte.RRH	Severity: minor Specific problem: OAM RRH FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-824 IK4009163

Alarm	Attributes	Applicable major release
Name: IK4009163 (3803) Type: equipmentAlarm Package: lte.IK4009163 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: OAM CB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-825 IK4009169

Alarm	Attributes	Applicable major release
Name: IK4009169 (3809) Type: equipmentAlarm Package: lte.IK4009169 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: END OF THE HOLDOVER DURATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that when it is close to the end of the holdover duration of the internal oscillator		

Table 29-825 IK4009169 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-826 IK4009171

Alarm	Attributes	Applicable major release
Name: IK4009171 (3810) Type: equipmentAlarm Package: lte.IK4009171 Raised on class: lte.RFM	Severity: minor Specific problem: ADAPTIVE ANTENNA ARRAY PARAMETER UPDATE FAILED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a cell Adaptive Antenna Array parameter has been changed but the RFM supporting the cell failed to implement the new value.		
Remedial action: Determine the alarm reason and remedy as necessary.		

Table 29-827 IK4009172

Alarm	Attributes	Applicable major release
Name: IK4009172 (3811) Type: equipmentAlarm Package: lte.IK4009172 Raised on class: lte.RFM	Severity: major Specific problem: ADAPTIVE ANTENNA ARRAY OPERATION DEGRADED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a hardware fault within the AAA function of the RFM is degrading the beam pattern.		
Remedial action: Replace the RFM hardware.		

Table 29-828 IK4009173

Alarm	Attributes	Applicable major release
Name: IK4009173 (3812) Type: equipmentAlarm Package: lte.IK4009173 Raised on class: lte.RFM	Severity: major Specific problem: ADAPTIVE ANTENNA ARRAY OPERATION FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a hardware fault within the AAA function of the RFM has disabled the AAA function.		
Remedial action: Replace the RFM hardware.		

Table 29-829 IK4009174

Alarm	Attributes	Applicable major release
Name: IK4009174 (3993) Type: equipmentAlarm Package: lte.IK4009174 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: DHCP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to stop the DHCP client on the eNodeB network interface.		
Remedial action: No action is required.		

Table 29-830 IK4009175

Alarm	Attributes	Applicable major release
Name: IK4009175 (3994) Type: equipmentAlarm Package: lte.IK4009175 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: DHCP LEASE LOST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the DHCP client lost the lease of the DHCP server.		
Remedial action: No action is required.		

Table 29-831 IK4009176

Alarm	Attributes	Applicable major release
Name: IK4009176 (3995) Type: equipmentAlarm Package: lte.IK4009176 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK MANUAL TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback is manually stopped.		
Remedial action: No action is required.		

Table 29-832 IK4009177

Alarm	Attributes	Applicable major release
Name: IK4009177 (3996) Type: equipmentAlarm Package: lte.IK4009177 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK INACTIVITY PERIOD TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback stopped automatically due to inactivity for certain period.		

Table 29-832 IK4009177 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-833 IK4009178

Alarm	Attributes	Applicable major release
Name: IK4009178 (3997) Type: equipmentAlarm Package: lte.IK4009178 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK GUARD TIMER TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the IP loopback stopped automatically due to expiry of the guard timer.		
Remedial action: No action is required.		

Table 29-834 IK4009179

Alarm	Attributes	Applicable major release
Name: IK4009179 (3998) Type: equipmentAlarm Package: lte.IK4009179 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM SCB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-835 IK4009180

Alarm	Attributes	Applicable major release
Name: IK4009180 (3999) Type: equipmentAlarm Package: lte.IK4009180 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM SCB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-836 IK4009181

Alarm	Attributes	Applicable major release
Name: IK4009181 (4000) Type: equipmentAlarm Package: lte.IK4009181 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM SCB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-837 IK4009182

Alarm	Attributes	Applicable major release
Name: IK4009182 (4001) Type: equipmentAlarm Package: lte.IK4009182 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM MF EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-838 IK4009185

Alarm	Attributes	Applicable major release
Name: IK4009185 (4004) Type: equipmentAlarm Package: lte.IK4009185 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SNTP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to stop the SNTP client.		
Remedial action: No action is required.		

Table 29-839 IK4009186

Alarm	Attributes	Applicable major release
Name: IK4009186 (4005) Type: equipmentAlarm Package: lte.IK4009186 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SSH SERVER STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to stop the SSH server.		

Table 29-839 IK4009186 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-840 IK4009188

Alarm	Attributes	Applicable major release
Name: IK4009188 (4007) Type: equipmentAlarm Package: lte.IK4009188 Raised on class: lte.RFME	Severity: indeterminate Specific problem: OAM RFME EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-841 IK4009189

Alarm	Attributes	Applicable major release
Name: IK4009189 (4008) Type: equipmentAlarm Package: lte.IK4009189 Raised on class: lte.RFME	Severity: indeterminate Specific problem: OAM RFME EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-842 IK4009191

Alarm	Attributes	Applicable major release
Name: IK4009191 (4010) Type: equipmentAlarm Package: lte.IK4009191 Raised on class: lte.M3MmeTransportLayerAccess	Severity: major Specific problem: M3 SCTP ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the MME does not acknowledge the M3 association request from the MCE.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME.		

Table 29-843 IK4009192

Alarm	Attributes	Applicable major release
Name: IK4009192 (4011) Type: equipmentAlarm Package: lte.IK4009192 Raised on class: lte.M3MmeTransportLayerAccess	Severity: major Specific problem: M3 SCTP ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a M3 association fault between the eNodeB and the MME.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME. 3. Check there is at least one eMBMS configured cell		

Table 29-844 IK4009193

Alarm	Attributes	Applicable major release
Name: IK4009193 (4012) Type: equipmentAlarm Package: lte.IK4009193 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates that the eICIC functionality is limited due to clock drift.		
Remedial action: No action is required.		

Table 29-845 IK4009194

Alarm	Attributes	Applicable major release
Name: IK4009194 (4013) Type: equipmentAlarm Package: lte.IK4009194 Raised on class: lte.MODULE	Severity: minor Specific problem: LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates that the eICIC functionality is limited due to clock drift.		
Remedial action: No action is required.		

Table 29-846 IK4009198

Alarm	Attributes	Applicable major release
Name: IK4009198 (4680) Type: equipmentAlarm Package: lte.IK4009198 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB PTP DISCONTINUOUS SESSION LOCK FAIL Implicitly cleared: true Default probable cause: lossOfSignal	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-846 IK4009198 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates, when the 1588 client is configured to Discontinuous mode that the client failed to achieve Lock in the 1588 message transfer session. This alarm is inhibited when the 1588 message transfer is in Continuous mode.		
Remedial action: Investigate the link PDV impairment profile. Increase the length of the active 1588 message transfer session.		

Table 29-847 IK4009203

Alarm	Attributes	Applicable major release
Name: IK4009203 (4685) Type: equipmentAlarm Package: lte.IK4009203 Raised on class: lte.MODULE	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-848 IK4009204

Alarm	Attributes	Applicable major release
Name: IK4009204 (4686) Type: equipmentAlarm Package: lte.IK4009204 Raised on class: lte.RFME	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The controller can no longer communicate with this unit.		
Remedial action: Check the board connectivity.		

Table 29-849 IK4009205

Alarm	Attributes	Applicable major release
Name: IK4009205 (4687) Type: equipmentAlarm Package: lte.IK4009205 Raised on class: lte.RFME	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the self test of the module reported an error.		
Remedial action: Reset the eNB. If the alarm persists, replace the module.		

Table 29-850 IK4009209

Alarm	Attributes	Applicable major release
Name: IK4009209 (4688) Type: equipmentAlarm Package: lte.IK4009209 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The controller can no longer communicate with this unit.		
Remedial action: Check for connectivity with the board.		

Table 29-851 IK4009210

Alarm	Attributes	Applicable major release
Name: IK4009210 (4689) Type: equipmentAlarm Package: lte.IK4009210 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: HW SW CAPABILITY CHECK RADIOCACENB FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: There is a mismatch between MIM configuration data RadioCacEnb and HW reported capabilities detected.		
Remedial action: The operator has to check the MIM configuration of RadioCacEnb object and the installed Controller Type. The MIM configuration must be aligned to the capability of the HW.		

Table 29-852 IK4009211

Alarm	Attributes	Applicable major release
Name: IK4009211 (7983) Type: equipmentAlarm Package: lte.IK4009211 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TO BB LOSS OF USER PLANE INTERBOARD CONNECTIVITY FOR LEGACY ENB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of User Plane inter-board connectivity between this BB board and the peer BB board(s) indicated in the additional info.		
Remedial action: Reset the board where the alarm is raised,\nIf it does not clear the alarm, perform an eNodeB reset;\nIf it fails to recover, replace the board.		

Table 29-853 IK4009212

Alarm	Attributes	Applicable major release
Name: IK4009212 (7984) Type: equipmentAlarm Package: lte.IK4009212 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TO BB LOSS OF USER PLANE INTERBOARD CONNECTIVITY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of User Plane inter-board connectivity between this BB board and the peer BB board(s) indicated in the additional info.		
Remedial action: Reset the board where the alarm is raised,\nIf it does not clear the alarm, perform an eNodeB reset;\nIf it fails to recover, replace the board.		

Table 29-854 IK4009213

Alarm	Attributes	Applicable major release
Name: IK4009213 (7985) Type: equipmentAlarm Package: lte.IK4009213 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB TO CB LOSS OF USER PLANE INTERBOARD CONNECTIVITY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of User Plane inter-board connectivity between this BB board and the CB board indicated in the additional info.		
Remedial action: Reset the board where the alarm is raised,\nIf it does not clear the alarm, perform an eNodeB reset;\nIf it fails to recover, replace the board.		

Table 29-855 IK4009214

Alarm	Attributes	Applicable major release
Name: IK4009214 (7986) Type: equipmentAlarm Package: lte.IK4009214 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB LOSS OF USER PLANE INTERBOARD CONNECTIVITY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a loss of User Plane inter-board connectivity between this CB board and the peer BB board(s) indicated in the additional info.		
Remedial action: Reset the eNodeB,\nIf it fails to recover, replace the board.		

Table 29-856 IK4009215

Alarm	Attributes	Applicable major release
Name: IK4009215 (7987) Type: processingErrorAlarm Package: lte.IK4009215 Raised on class: lte.RFM	Severity: minor Specific problem: RFM TEMPORARY UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RFM cannot execute the request because it is temporary unavailable. The request will be repeated.		
Remedial action: No action is required		

Table 29-857 IK4009216

Alarm	Attributes	Applicable major release
Name: IK4009216 (7988) Type: processingErrorAlarm Package: lte.IK4009216 Raised on class: lte.RFM	Severity: critical Specific problem: RFM UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persist replace the module.		

Table 29-858 IK4009217

Alarm	Attributes	Applicable major release
Name: IK4009217 (7989) Type: processingErrorAlarm Package: lte.IK4009217 Raised on class: lte.RFM	Severity: major Specific problem: RFM PROCESSING ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to RFM failure of processing.		
Remedial action: Reset the module. If the alarm persist replace the module.		

Table 29-859 IK4009218

Alarm	Attributes	Applicable major release
Name: IK4009218 (7990) Type: processingErrorAlarm Package: lte.IK4009218 Raised on class: lte.RFM	Severity: major Specific problem: RFM NOT OPERATIONAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RFM has been detected as not operational. In most situations a second alarm related to this object should be already raised and an equipment reset already triggered.		

Table 29-859 IK4009218 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the eNodeB recovery action does not fix the alarm then reset the module. If the alarm persists replace the module.		

Table 29-860 IK4009219

Alarm	Attributes	Applicable major release
Name: IK4009219 (8664) Type: equipmentAlarm Package: lte.IK4009219 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: OAM BB EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-861 IK4009220

Alarm	Attributes	Applicable major release
Name: IK4009220 (8665) Type: equipmentAlarm Package: lte.IK4009220 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: OAM CB FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-862 IK4009221

Alarm	Attributes	Applicable major release
Name: IK4009221 (8666) Type: equipmentAlarm Package: lte.IK4009221 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: OAM CB FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-863 IK4009222

Alarm	Attributes	Applicable major release
Name: IK4009222 (8667) Type: equipmentAlarm Package: lte.IK4009222 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-864 IK4009223

Alarm	Attributes	Applicable major release
Name: IK4009223 (8668) Type: equipmentAlarm Package: lte.IK4009223 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-865 IK4009224

Alarm	Attributes	Applicable major release
Name: IK4009224 (8669) Type: equipmentAlarm Package: lte.IK4009224 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OAM ENB FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-866 IK4009225

Alarm	Attributes	Applicable major release
Name: IK4009225 (8670) Type: equipmentAlarm Package: lte.IK4009225 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OAM ENB FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		

Table 29-866 IK4009225 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Call the next level of support.		

Table 29-867 IK4009226

Alarm	Attributes	Applicable major release
Name: IK4009226 (8671) Type: equipmentAlarm Package: lte.IK4009226 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OAM ENB FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-868 IK4009227

Alarm	Attributes	Applicable major release
Name: IK4009227 (8672) Type: equipmentAlarm Package: lte.IK4009227 Raised on class: lte.ENBEquipment	Severity: major Specific problem: OAM ENB FAULT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-869 IK4009228

Alarm	Attributes	Applicable major release
Name: IK4009228 (8673) Type: equipmentAlarm Package: lte.IK4009228 Raised on class: lte.ENBEquipment	Severity: major Specific problem: OAM ENB FAULT 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-870 IK4009229

Alarm	Attributes	Applicable major release
Name: IK4009229 (8674) Type: equipmentAlarm Package: lte.IK4009229 Raised on class: lte.TRDU	Severity: minor Specific problem: OAM TRDU FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-871 IK4009230

Alarm	Attributes	Applicable major release
Name: IK4009230 (8675) Type: equipmentAlarm Package: lte.IK4009230 Raised on class: lte.TRDU	Severity: minor Specific problem: OAM TRDU FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-872 IK4009231

Alarm	Attributes	Applicable major release
Name: IK4009231 (8676) Type: equipmentAlarm Package: lte.IK4009231 Raised on class: lte.TRDU	Severity: major Specific problem: OAM TRDU FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-873 IK4009232

Alarm	Attributes	Applicable major release
Name: IK4009232 (8677) Type: equipmentAlarm Package: lte.IK4009232 Raised on class: lte.RRH	Severity: minor Specific problem: OAM RRH FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-873 IK4009232 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-874 IK4009233

Alarm	Attributes	Applicable major release
Name: IK4009233 (8678) Type: equipmentAlarm Package: lte.IK4009233 Raised on class: lte.RRH	Severity: minor Specific problem: OAM RRH FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-875 IK4009234

Alarm	Attributes	Applicable major release
Name: IK4009234 (8679) Type: equipmentAlarm Package: lte.IK4009234 Raised on class: lte.RRH	Severity: major Specific problem: OAM RRH FAULT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-876 IK4009235

Alarm	Attributes	Applicable major release
Name: IK4009235 (8680) Type: equipmentAlarm Package: lte.IK4009235 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM MF EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-877 IK4009236

Alarm	Attributes	Applicable major release
Name: IK4009236 (8681) Type: equipmentAlarm Package: lte.IK4009236 Raised on class: lte.RFME	Severity: indeterminate Specific problem: OAM RFME EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-878 IK4009237

Alarm	Attributes	Applicable major release
Name: IK4009237 (8682) Type: equipmentAlarm Package: lte.IK4009237 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: OAM ENB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-879 IK4009238

Alarm	Attributes	Applicable major release
Name: IK4009238 (8683) Type: equipmentAlarm Package: lte.IK4009238 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: OAM ENB EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-880 IK4009239

Alarm	Attributes	Applicable major release
Name: IK4009239 (8684) Type: equipmentAlarm Package: lte.IK4009239 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: OAM ENB EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		

Table 29-880 IK4009239 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-881 IK4009240

Alarm	Attributes	Applicable major release
Name: IK4009240 (8685) Type: equipmentAlarm Package: lte.IK4009240 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OAM ENB EVENT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-882 IK4009241

Alarm	Attributes	Applicable major release
Name: IK4009241 (8686) Type: equipmentAlarm Package: lte.IK4009241 Raised on class: lte.RRH	Severity: minor Specific problem: PATH DELAY MEASUREMENT FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that one or more of the Path Delay Measurements were outside the range of values.		
Remedial action: Check the Return Loss value and if it is not greater than 14 dB, there is a problem in one or more of the RF paths supported by the RRH. If the Return Loss value is greater than 14 dB, the RRH might have to be replaced. If the alarm persists after a reset of the RRH, contact the next level of support.		

Table 29-883 IK4009242

Alarm	Attributes	Applicable major release
Name: IK4009242 (8687) Type: equipmentAlarm Package: lte.IK4009242 Raised on class: lte.TRDU	Severity: minor Specific problem: PATH DELAY MEASUREMENT FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that one or more of the Path Delay Measurements were outside the range of values.		
Remedial action: Check the Return Loss value and if it is not greater than 14 dB, there is a problem in one or more of the RF paths supported by the TRDU. If the Return Loss value is greater than 14 dB, the TRDU might have to be replaced. If the alarm persists after a reset of the TRDU, contact the next level of support.		

Table 29-884 IK4009243

Alarm	Attributes	Applicable major release
Name: IK4009243 (8688) Type: equipmentAlarm Package: lte.IK4009243 Raised on class: lte.Rco2TransportLayerAccess	Severity: major Specific problem: CS-VNF SCTP ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the CS-VNF does not acknowledge the CS-VNF association requests from the eNodeB.		
Remedial action: Reset the eNodeB.		

Table 29-885 IK4009244

Alarm	Attributes	Applicable major release
Name: IK4009244 (8689) Type: equipmentAlarm Package: lte.IK4009244 Raised on class: lte.Rco2TransportLayerAccess	Severity: major Specific problem: CS-VNF SCTP ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a fault in the RCo2 association between the eNodeBs and CS-VNF.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and CS-VNF. 2. Check network connectivity between eNB and CS-VNF.		

Table 29-886 IK4009246

Alarm	Attributes	Applicable major release
Name: IK4009246 (8690) Type: equipmentAlarm Package: lte.IK4009246 Raised on class: lte.RRH	Severity: minor Specific problem: TTLNA GAIN IS OUTSIDE RRH/TRDU CAPABILIYAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RRH cannot compensate for the RF Gain of the TMA that is assigned to its transmit port.		
Remedial action: Set the TMA gain to a value that can be supported by the RRH. Contact the next level of support.		

Table 29-887 IK4009247

Alarm	Attributes	Applicable major release
Name: IK4009247 (8691) Type: qualityOfServiceAlarm Package: lte.IK4009247 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.ENBEquipment • lte.MODULE • lte.RRH	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-888 IK4009248

Alarm	Attributes	Applicable major release
Name: IK4009248 (8692) Type: processingErrorAlarm Package: lte.IK4009248 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RAM USAGE OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the RAM exhausted.		
Remedial action: No action is required.		

Table 29-889 IK4009249

Alarm	Attributes	Applicable major release
Name: IK4009249 (8693) Type: processingErrorAlarm Package: lte.IK4009249 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: PROCESSING UNIT OCCUPANCY OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-889 IK4009249 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the processing unit is overloaded.		
Remedial action: No action is required.		

Table 29-890 IK4009250

Alarm	Attributes	Applicable major release
Name: IK4009250 (8694) Type: equipmentAlarm Package: lte.IK4009250 Raised on classes: • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.AMR • lte.TmaAldEntry • lte.RRH	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-891 IK4009251

Alarm	Attributes	Applicable major release
Name: IK4009251 (8695) Type: processingErrorAlarm Package: lte.IK4009251 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RFME • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.TmaAldEntry • lte.AMR • lte.RRH	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the time-out for a response from the module.		

Table 29-891 IK4009251 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-892 IK4009252

Alarm	Attributes	Applicable major release
Name: IK4009252 (8696) Type: equipmentAlarm Package: lte.IK4009252 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.ENBEquipment • lte.MODULE • lte.RRH	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-893 IK4009253

Alarm	Attributes	Applicable major release
Name: IK4009253 (8697) Type: equipmentAlarm Package: lte.IK4009253 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: WALG INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to initialize the WAL gateway.		
Remedial action: Reset the eNodeB.		

Table 29-894 IK4009255

Alarm	Attributes	Applicable major release
Name: IK4009255 (8698) Type: equipmentAlarm Package: lte.IK4009255 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.RRH	Severity: critical Specific problem: AUTOTEST FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the self test of the module reported an error or that a software download or software activation did not succeed.		
Remedial action: Reset the module. If the alarm persists, redo the software download and software activation. If unsuccessful, replace the module.		

Table 29-895 IK4009256

Alarm	Attributes	Applicable major release
Name: IK4009256 (8699) Type: equipmentAlarm Package: lte.IK4009256 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK GUARD TIMER TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the IP loopback stopped automatically due to expiry of the guard timer.		
Remedial action: No action is required.		

Table 29-896 IK4009257

Alarm	Attributes	Applicable major release
Name: IK4009257 (8700) Type: equipmentAlarm Package: lte.IK4009257 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK INACTIVITY PERIOD TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-896 IK4009257 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the IP loopback stopped automatically due to inactivity for certain period.		
Remedial action: No action is required.		

Table 29-897 IK4009258

Alarm	Attributes	Applicable major release
Name: IK4009258 (8701) Type: equipmentAlarm Package: lte.IK4009258 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: IP LOOPBACK MANUAL TERMINATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the IP loopback is manually stopped.		
Remedial action: No action is required.		

Table 29-898 IK4009259

Alarm	Attributes	Applicable major release
Name: IK4009259 (8702) Type: equipmentAlarm Package: lte.IK4009259 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: IP LOOPBACK ACTIVE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the IP loopback is activated.		
Remedial action: Call the next level of support.		

Table 29-899 IK4009260

Alarm	Attributes	Applicable major release
Name: IK4009260 (8703) Type: equipmentAlarm Package: lte.IK4009260 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: DHCP CLIENT LEASE FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-899 IK4009260 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure of the DHCP client to obtain the lease from the DHCP server.		
Remedial action: Check for connectivity. Check for DHCP server and network configurations.		

Table 29-900 IK4009261

Alarm	Attributes	Applicable major release
Name: IK4009261 (8704) Type: equipmentAlarm Package: lte.IK4009261 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: DHCP LEASE LOST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the DHCP client lost the lease of the DHCP server.		
Remedial action: No action is required.		

Table 29-901 IK4009262

Alarm	Attributes	Applicable major release
Name: IK4009262 (8705) Type: equipmentAlarm Package: lte.IK4009262 Raised on classes: • lte.RFME • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.ENBEquipment • lte.TmaAldEntry • lte.AMR • lte.RRH	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check the board connectivity.		

Table 29-902 IK4009263

Alarm	Attributes	Applicable major release
Name: IK4009263 (8706) Type: communicationsAlarm Package: lte.IK4009263 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: ETHERNET TRANSPORT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an interface error due to the counters exceeding the configured threshold.		
Remedial action: Check the network status and cabling if possible. If the alarm persists, contact the next level support.		

Table 29-903 IK4009264

Alarm	Attributes	Applicable major release
Name: IK4009264 (8707) Type: processingErrorAlarm Package: lte.IK4009264 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: UNEXPECTED DATA FROM DHCP SERVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the lease time offered by the DHCP server is different from the lease time requested by the DHCP client.		
Remedial action: Configure the DHCP server with an infinite lease time.		

Table 29-904 IK4009265

Alarm	Attributes	Applicable major release
Name: IK4009265 (8708) Type: equipmentAlarm Package: lte.IK4009265 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: DHCP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to stop the DHCP client on the eNodeB network interface.		
Remedial action: No action is required.		

Table 29-905 IK4009266

Alarm	Attributes	Applicable major release
Name: IK4009266 (8709) Type: equipmentAlarm Package: lte.IK4009266 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: SNTP CLIENT STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to stop the SNTP client.		
Remedial action: No action is required.		

Table 29-906 IK4009267

Alarm	Attributes	Applicable major release
Name: IK4009267 (8710) Type: equipmentAlarm Package: lte.IK4009267 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: DHCP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to start the DHCP client on the eNodeB network interface.		
Remedial action: Reset the eNodeB.		

Table 29-907 IK4009268

Alarm	Attributes	Applicable major release
Name: IK4009268 (8711) Type: equipmentAlarm Package: lte.IK4009268 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: SNTP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to start the SNTP client.		
Remedial action: Check the network connectivity of NTP server and NTP server address provisioning. If the NTP server is unreachable or the provisioning is incorrect, address those aspects. If all other possible causes have been eliminated, reset the eNB.		

Table 29-908 IK4009269

Alarm	Attributes	Applicable major release
Name: IK4009269 (8712) Type: equipmentAlarm Package: lte.IK4009269 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: SSH SERVER STOP FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to stop the SSH server.		
Remedial action: No action is required.		

Table 29-909 IK4009270

Alarm	Attributes	Applicable major release
Name: IK4009270 (8713) Type: equipmentAlarm Package: lte.IK4009270 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: SSH SERVER START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to start the SSH server.		
Remedial action: Reset the eNodeB.		

Table 29-910 IK4009271

Alarm	Attributes	Applicable major release
Name: IK4009271 (8714) Type: equipmentAlarm Package: lte.IK4009271 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: TELECOM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the telecom interface.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-911 IK4009272

Alarm	Attributes	Applicable major release
Name: IK4009272 (8715) Type: equipmentAlarm Package: lte.IK4009272 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: OAM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the OAM interface.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-912 IK4009273

Alarm	Attributes	Applicable major release
Name: IK4009273 (8716) Type: equipmentAlarm Package: lte.IK4009273 Raised on classes: • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.TmaAldEntry • lte.AMR • lte.RRH	Severity: indeterminate Specific problem: MODULE EXTRACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the system detected extraction of the module.		
Remedial action: No action is required.		

Table 29-913 IK4009275

Alarm	Attributes	Applicable major release
Name: IK4009275 (8717) Type: equipmentAlarm Package: lte.IK4009275 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: END POINTS ALLOCATION MISMATCH Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This is an event , which notifies, in a non-cross connect configuration, a misalignment between database defined UL/DL antennas and actual requested UL/DL antennas (radio endpoints) The above EVENT has meaning IF IT isn't associated with alarms representing: * different MISMATCH conditions; * HW SW capability check conditions when UL/DL antennas downgrade is an expected result.		

Table 29-913 IK4009275 (continued)

Alarm	Attributes	Applicable major release
Remedial action: In cases where the event has meaning (see DESCRIPTION), perform the following actions sequence (in that order): 1. Save persistently the OAM-C detailed code traces (running log should be already stopped, due to the above event) 2. In order to remove faulty condition: * cell lock-unlock; * eNB reset		

Table 29-914 IK4009276

Alarm	Attributes	Applicable major release
Name: IK4009276 (8718) Type: communicationsAlarm Package: lte.IK4009276 Raised on class: lte.MmeAccess	Severity: critical Specific problem: NO RESPONSE TO GTP ECHO REQUEST ON S1U Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the last S1 fault following no response to a GTP Echo request.\nThe alarm is triggered when the eNodeB does not receive a response to a GTP echo request message sent on a S1 interface towards a Serving Gateway. The alarm is triggered to signal a S1 failure when there are several SGW because of several operators with their own SGW or because an operator has several SGW. It is not possible to identify the failed S1 link.		
Remedial action: Check for connectivity and verify the GTP provisioning.		

Table 29-915 IK4009277

Alarm	Attributes	Applicable major release
Name: IK4009277 (8719) Type: equipmentAlarm Package: lte.IK4009277 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: SCTP INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to initialize the SCTP access.		
Remedial action: Reset the eNodeB.		

Table 29-916 IK4009278

Alarm	Attributes	Applicable major release
Name: IK4009278 (10083) Type: communicationsAlarm Package: lte.IK4009278 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: OAM CB FAULT 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		

Table 29-916 IK4009278 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the additional information for maintenance action details.		

Table 29-917 IK4009279

Alarm	Attributes	Applicable major release
Name: IK4009279 (10084) Type: communicationsAlarm Package: lte.IK4009279 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: OAM CB FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-918 IK4009280

Alarm	Attributes	Applicable major release
Name: IK4009280 (10085) Type: processingErrorAlarm Package: lte.IK4009280 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: OAM CB FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-919 IK4009281

Alarm	Attributes	Applicable major release
Name: IK4009281 (10086) Type: processingErrorAlarm Package: lte.IK4009281 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: OAM CB FAULT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-920 IK4009282

Alarm	Attributes	Applicable major release
Name: IK4009282 (10087) Type: processingErrorAlarm Package: lte.IK4009282 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 8 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-921 IK4009283

Alarm	Attributes	Applicable major release
Name: IK4009283 (10088) Type: equipmentAlarm Package: lte.IK4009283 Raised on class: lte.RFM	Severity: minor Specific problem: TTLNA GAIN IS OUTSIDE RRH/TRDU CAPABILITY Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RFM cannot compensate for the RF Gain of the TMA that is assigned to its receive port or the value entered in the parameter ttlnaAntennaGain.		
Remedial action: Set the TMA gain to a value that can be supported by the RRH using the parameter tmaSubunitRfGainConfigure\non the TmaSubunit object properties or change the value in the parameter ttlnaAntennaGain. Contact the next level of support if problem persists.		

Table 29-922 IK4009290

Alarm	Attributes	Applicable major release
Name: IK4009290 (10089) Type: equipmentAlarm Package: lte.IK4009290 Raised on class: lte.Rae	Severity: minor Specific problem: OAM RAE FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-923 IK4009291

Alarm	Attributes	Applicable major release
Name: IK4009291 (10090) Type: equipmentAlarm Package: lte.IK4009291 Raised on class: lte.Rae	Severity: major Specific problem: OAM RAE FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-924 IK4009292

Alarm	Attributes	Applicable major release
Name: IK4009292 (10091) Type: equipmentAlarm Package: lte.IK4009292 Raised on class: lte.Rae	Severity: major Specific problem: OAM RAE FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-925 IK4009293

Alarm	Attributes	Applicable major release
Name: IK4009293 (10092) Type: equipmentAlarm Package: lte.IK4009293 Raised on class: lte.Rae	Severity: indeterminate Specific problem: OAM RAE EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-926 IK4009294

Alarm	Attributes	Applicable major release
Name: IK4009294 (10093) Type: equipmentAlarm Package: lte.IK4009294 Raised on class: lte.Rae	Severity: indeterminate Specific problem: OAM RAE EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-927 IK4009295

Alarm	Attributes	Applicable major release
Name: IK4009295 (10094) Type: equipmentAlarm Package: lte.IK4009295 Raised on class: lte.Rae	Severity: indeterminate Specific problem: OAM RAE EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-928 IK4009296

Alarm	Attributes	Applicable major release
Name: IK4009296 (10095) Type: equipmentAlarm Package: lte.IK4009296 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-929 IK4009297

Alarm	Attributes	Applicable major release
Name: IK4009297 (10096) Type: equipmentAlarm Package: lte.IK4009297 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-930 IK4009298

Alarm	Attributes	Applicable major release
Name: IK4009298 (10097) Type: processingErrorAlarm Package: lte.IK4009298 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-931 IK4009299

Alarm	Attributes	Applicable major release
Name: IK4009299 (10098) Type: qualityOfServiceAlarm Package: lte.IK4009299 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 6 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-932 IK4009300

Alarm	Attributes	Applicable major release
Name: IK4009300 (10099) Type: processingErrorAlarm Package: lte.IK4009300 Raised on class: lte.RFM	Severity: major Specific problem: OAM RFM FAULT 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Unknown.		

Table 29-933 IK4009301

Alarm	Attributes	Applicable major release
Name: IK4009301 (10100) Type: processingErrorAlarm Package: lte.IK4009301 Raised on class: lte.RFM	Severity: major Specific problem: OAM RFM FAULT 11/SECONDARY MODE Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-934 IK4009302

Alarm	Attributes	Applicable major release
Name: IK4009302 (10101) Type: processingErrorAlarm Package: lte.IK4009302 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 7/SECONDARY MODE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		

Table 29-934 IK4009302 (continued)

Alarm	Attributes	Applicable major release
Remedial action: None.		

Table 29-935 IK4009306

Alarm	Attributes	Applicable major release
Name: IK4009306 (10102) Type: equipmentAlarm Package: lte.IK4009306 Raised on class: lte.RFM	Severity: minor Specific problem: RFM - INPUT DC VOLTAGE BELOW MINIMUM THRESHOLD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the DC input voltage to the RFM (RRH/TRDU) is below the minimum threshold for the RRH or TRDU.		
Remedial action: None.		

Table 29-936 IK4009316

Alarm	Attributes	Applicable major release
Name: IK4009316 (10103) Type: processingErrorAlarm Package: lte.IK4009316 Raised on classes: • lte.RFM • lte.CBCardSpecifics	Severity: major Specific problem: MODULE TEMPORARY UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the module cannot execute the request because it is temporary unavailable. The request will be repeated.		
Remedial action: No action is required		

Table 29-937 IK4009317

Alarm	Attributes	Applicable major release
Name: IK4009317 (10104) Type: processingErrorAlarm Package: lte.IK4009317 Raised on classes: • lte.RFM • lte.CBCardSpecifics	Severity: critical Specific problem: MODULE UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the scenario failure due to no-response from the module.		

Table 29-937 IK4009317 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the module. If the alarm persist replace the module.		

Table 29-938 IK4009318

Alarm	Attributes	Applicable major release
Name: IK4009318 (10105) Type: processingErrorAlarm Package: lte.IK4009318 Raised on classes: • lte.RFM • lte.CBCardSpecifics	Severity: major Specific problem: MODULE PROCESSING ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the scenario failed due to module failure during the processing.		
Remedial action: Reset the module. If the alarm persist replace the module.		

Table 29-939 IK4009319

Alarm	Attributes	Applicable major release
Name: IK4009319 (10106) Type: processingErrorAlarm Package: lte.IK4009319 Raised on classes: • lte.RFM • lte.CBCardSpecifics	Severity: major Specific problem: MODULE NOT OPERATIONAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the module has been detected as not operational. In most situations a second alarm related to this object should be already raised and an equipment reset already triggered.		
Remedial action: If the eNodeB recovery action does not fix the alarm then reset the module. If the alarm persists replace the module.		

Table 29-940 IK4009320

Alarm	Attributes	Applicable major release
Name: IK4009320 (10107) Type: equipmentAlarm Package: lte.IK4009320 Raised on classes: • lte.RFM • lte.RFME • lte.RetAldEntry • lte.BBCardSpecifics • lte.ENBEquipment • lte.AMR • lte.Rae • lte.TmaAldEntry	Severity: major Specific problem: NO CONTACT TO BOARD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure in communication with the board.		
Remedial action: Check the board connectivity.		

Table 29-941 IK4009321

Alarm	Attributes	Applicable major release
Name: IK4009321 (11016) Type: equipmentAlarm Package: lte.IK4009321 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: OAM ENB EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-942 IK4009324

Alarm	Attributes	Applicable major release
Name: IK4009324 (11017) Type: equipmentAlarm Package: lte.IK4009324 Raised on class: lte.MODULE	Severity: minor Specific problem: RADIO CAC NOT SUPPORTED BY HW Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: There is a mismatch between MIM configuration data RadioCacEnb and HW reported capabilities detected.		
Remedial action: The operator has to check the MIM configuration of RadioCacEnb object and the installed Controller Type. The MIM configuration must be aligned to the capability of the HW.		

Table 29-943 IK4009325

Alarm	Attributes	Applicable major release
Name: IK4009325 (11018) Type: qualityOfServiceAlarm Package: lte.IK4009325 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.ENBEquipment • lte.RRH	Severity: indeterminate Specific problem: DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-944 IK4009326

Alarm	Attributes	Applicable major release
Name: IK4009326 (11019) Type: qualityOfServiceAlarm Package: lte.IK4009326 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DEBUG SESSION ON-DEMAND SNAPSHOT FILE AVAILABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates the availability of new on-demand snapshot files.		
Remedial action: No action is required.		

Table 29-945 IK4009327

Alarm	Attributes	Applicable major release
Name: IK4009327 (11020) Type: qualityOfServiceAlarm Package: lte.IK4009327 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DEBUG SESSION ON-DEMAND SNAPSHOT UPLOAD FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the transfer of the new on-demand snapshot files to the target server failed.		
Remedial action: No action is required.		

Table 29-946 IK4010001

Alarm	Attributes	Applicable major release
Name: IK4010001 (2664) Type: equipmentAlarm Package: lte.IK4010001 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to read manufacturer data record.		
Remedial action: Reset the RET, replace if necessary.		

Table 29-947 IK4010002

Alarm	Attributes	Applicable major release
Name: IK4010002 (2665) Type: equipmentAlarm Package: lte.IK4010002 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET actuator.		

Table 29-948 IK4010003

Alarm	Attributes	Applicable major release
Name: IK4010003 (2666) Type: equipmentAlarm Package: lte.IK4010003 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET actuator.		

Table 29-949 IK4010004

Alarm	Attributes	Applicable major release
Name: IK4010004 (2667) Type: equipmentAlarm Package: lte.IK4010004 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-949 IK4010004 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RET device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET calibration procedure.		

Table 29-950 IK4010005

Alarm	Attributes	Applicable major release
Name: IK4010005 (2668) Type: equipmentAlarm Package: lte.IK4010005 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data and repeat calibration.		

Table 29-951 IK4010006

Alarm	Attributes	Applicable major release
Name: IK4010006 (2669) Type: equipmentAlarm Package: lte.IK4010006 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET HW FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a general hardware failure.		
Remedial action: Reset the RET, replace the RET if the problem persists.		

Table 29-952 IK4010007

Alarm	Attributes	Applicable major release
Name: IK4010007 (2670) Type: equipmentAlarm Package: lte.IK4010007 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET unit. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-953 IK4010008

Alarm	Attributes	Applicable major release
Name: IK4010008 (2671) Type: equipmentAlarm Package: lte.IK4010008 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SOFTWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a general RET SW failure.		
Remedial action: Reset the RET. If the problem persists then download new software to the RET, otherwise replace the RET.		

Table 29-954 IK4010009

Alarm	Attributes	Applicable major release
Name: IK4010009 (2672) Type: equipmentAlarm Package: lte.IK4010009 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ALD UNIT SUPPORT WRONG AISG VERSION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the ALD unit does not support AISG version 2.0.		
Remedial action: Upgrade the software.		

Table 29-955 IK4010010

Alarm	Attributes	Applicable major release
Name: IK4010010 (2673) Type: equipmentAlarm Package: lte.IK4010010 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET LOSS OF COMM Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L
Description: This alarm indicates the RFM that acts as an AISG Controller lost communication to the RET unit.		
Remedial action: Inspect and repair the AISG bus if needed, otherwise replace the RET.		

Table 29-956 IK4010012

Alarm	Attributes	Applicable major release
Name: IK4010012 (3206) Type: equipmentAlarm Package: lte.IK4010012 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified RET fault.		

Table 29-956 IK4010012 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the additional info for maintenance action details.		

Table 29-957 IK4010013

Alarm	Attributes	Applicable major release
Name: IK4010013 (3207) Type: equipmentAlarm Package: lte.IK4010013 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RET fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-958 IK4010014

Alarm	Attributes	Applicable major release
Name: IK4010014 (3208) Type: equipmentAlarm Package: lte.IK4010014 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RET fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-959 IK4010015

Alarm	Attributes	Applicable major release
Name: IK4010015 (3209) Type: equipmentAlarm Package: lte.IK4010015 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RET fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-960 IK4010017

Alarm	Attributes	Applicable major release
Name: IK4010017 (3814) Type: equipmentAlarm Package: lte.IK4010017 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 2 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 2 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 2 actuator.		

Table 29-961 IK4010018

Alarm	Attributes	Applicable major release
Name: IK4010018 (3815) Type: equipmentAlarm Package: lte.IK4010018 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 2 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 2 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 2 actuator.		

Table 29-962 IK4010019

Alarm	Attributes	Applicable major release
Name: IK4010019 (3816) Type: equipmentAlarm Package: lte.IK4010019 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 2 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 2 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET Subunit 2 calibration procedure.		

Table 29-963 IK4010020

Alarm	Attributes	Applicable major release
Name: IK4010020 (3817) Type: equipmentAlarm Package: lte.IK4010020 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 2 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-963 IK4010020 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RET Subunit 2 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to Subunit 2 and repeat calibration.		

Table 29-964 IK4010021

Alarm	Attributes	Applicable major release
Name: IK4010021 (3818) Type: equipmentAlarm Package: lte.IK4010021 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 3 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 3 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 3 actuator.		

Table 29-965 IK4010022

Alarm	Attributes	Applicable major release
Name: IK4010022 (3819) Type: equipmentAlarm Package: lte.IK4010022 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 3 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 3 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 3 actuator.		

Table 29-966 IK4010023

Alarm	Attributes	Applicable major release
Name: IK4010023 (3820) Type: equipmentAlarm Package: lte.IK4010023 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 3 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 3 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET calibration procedure for Subunit 3.		

Table 29-967 IK4010024

Alarm	Attributes	Applicable major release
Name: IK4010024 (3821) Type: equipmentAlarm Package: lte.IK4010024 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 3 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 3 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to subunit 3 and repeat calibration.		

Table 29-968 IK4010025

Alarm	Attributes	Applicable major release
Name: IK4010025 (3822) Type: equipmentAlarm Package: lte.IK4010025 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 4 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 4 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 4 actuator.		

Table 29-969 IK4010026

Alarm	Attributes	Applicable major release
Name: IK4010026 (3823) Type: equipmentAlarm Package: lte.IK4010026 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 4 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 4 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 4 actuator.		

Table 29-970 IK4010027

Alarm	Attributes	Applicable major release
Name: IK4010027 (3824) Type: equipmentAlarm Package: lte.IK4010027 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 4 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-970 IK4010027 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RET Subunit 4 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET Subunit 4 calibration procedure.		

Table 29-971 IK4010028

Alarm	Attributes	Applicable major release
Name: IK4010028 (3825) Type: equipmentAlarm Package: lte.IK4010028 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 4 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 4 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to Subunit 4 and repeat calibration.		

Table 29-972 IK4010029

Alarm	Attributes	Applicable major release
Name: IK4010029 (4014) Type: equipmentAlarm Package: lte.IK4010029 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET subunit 1. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-973 IK4010030

Alarm	Attributes	Applicable major release
Name: IK4010030 (4015) Type: equipmentAlarm Package: lte.IK4010030 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET subunit 2. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-974 IK4010031

Alarm	Attributes	Applicable major release
Name: IK4010031 (4016) Type: equipmentAlarm Package: lte.IK4010031 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET subunit 3. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-975 IK4010032

Alarm	Attributes	Applicable major release
Name: IK4010032 (4017) Type: equipmentAlarm Package: lte.IK4010032 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET subunit 4. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-976 IK4010033

Alarm	Attributes	Applicable major release
Name: IK4010033 (4018) Type: equipmentAlarm Package: lte.IK4010033 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 1 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 1 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 1 actuator.		

Table 29-977 IK4010034

Alarm	Attributes	Applicable major release
Name: IK4010034 (4019) Type: equipmentAlarm Package: lte.IK4010034 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 1 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 1 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 1 actuator.		

Table 29-978 IK4010035

Alarm	Attributes	Applicable major release
Name: IK4010035 (4020) Type: equipmentAlarm Package: lte.IK4010035 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 1 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 1 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET Subunit 1 calibration procedure.		

Table 29-979 IK4010036

Alarm	Attributes	Applicable major release
Name: IK4010036 (4021) Type: equipmentAlarm Package: lte.IK4010036 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 1 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 1 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to Subunit 1 and repeat calibration.		

Table 29-980 IK4010038

Alarm	Attributes	Applicable major release
Name: IK4010038 (4690) Type: equipmentAlarm Package: lte.IK4010038 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: ALL SUBUNITS IN ALARM STATUS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-980 IK4010038 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that all the subunits (or the only unit of a single subunit device) are in alarm.		
Remedial action: Refer to the alarm reported for the specific subunits and correct the fault or replace the unit as necessary.		

Table 29-981 IK4010039

Alarm	Attributes	Applicable major release
Name: IK4010039 (5238) Type: equipmentAlarm Package: lte.IK4010039 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a failure of the RET has been detected that cannot described by any specific alarm.		
Remedial action: The unit is automatically reset to attempt to clear the fault. If the problem persists then replace the RET.		

Table 29-982 IK4010040

Alarm	Attributes	Applicable major release
Name: IK4010040 (8720) Type: equipmentAlarm Package: lte.IK4010040 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RET fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-983 IK4010041

Alarm	Attributes	Applicable major release
Name: IK4010041 (8721) Type: equipmentAlarm Package: lte.IK4010041 Raised on class: lte.RetAldEntry	Severity: major Specific problem: RET FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RET fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-984 IK4010042

Alarm	Attributes	Applicable major release
Name: IK4010042 (8722) Type: equipmentAlarm Package: lte.IK4010042 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: minor Specific problem: ALD UNIT SUPPORT WRONG AISG VERSION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the ALD unit does not support AISG version 2.0.		
Remedial action: Upgrade the software.		

Table 29-985 IK4010043

Alarm	Attributes	Applicable major release
Name: IK4010043 (8723) Type: equipmentAlarm Package: lte.IK4010043 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 5 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 5 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET Subunit 5 calibration procedure.		

Table 29-986 IK4010044

Alarm	Attributes	Applicable major release
Name: IK4010044 (8724) Type: equipmentAlarm Package: lte.IK4010044 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 6 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 6 device has not completed a calibration operation, or calibration has been lost		
Remedial action: Execute the RET Subunit 6 calibration procedure.		

Table 29-987 IK4010045

Alarm	Attributes	Applicable major release
Name: IK4010045 (8725) Type: equipmentAlarm Package: lte.IK4010045 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 5 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 5 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to Subunit 5 and repeat calibration.		

Table 29-988 IK4010046

Alarm	Attributes	Applicable major release
Name: IK4010046 (8726) Type: equipmentAlarm Package: lte.IK4010046 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 6 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 6 actuator antenna configuration file is missing.		
Remedial action: Download proper ACF configuration data to Subunit 6 and repeat calibration.		

Table 29-989 IK4010047

Alarm	Attributes	Applicable major release
Name: IK4010047 (8727) Type: equipmentAlarm Package: lte.IK4010047 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an actuator movement outside the control of the RET subunit 5. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-990 IK4010048

Alarm	Attributes	Applicable major release
Name: IK4010048 (8728) Type: equipmentAlarm Package: lte.IK4010048 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ACTUATOR INTERFERENCE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-990 IK4010048 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates an actuator movement outside the control of the RET subunit 6. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-991 IK4010049

Alarm	Attributes	Applicable major release
Name: IK4010049 (8729) Type: equipmentAlarm Package: lte.IK4010049 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 5 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 5 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 5 actuator.		

Table 29-992 IK4010050

Alarm	Attributes	Applicable major release
Name: IK4010050 (8730) Type: equipmentAlarm Package: lte.IK4010050 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 6 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RET Subunit 6 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 6 actuator.		

Table 29-993 IK4010051

Alarm	Attributes	Applicable major release
Name: IK4010051 (8731) Type: equipmentAlarm Package: lte.IK4010051 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 5 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 5 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 5 actuator.		

Table 29-994 IK4010052

Alarm	Attributes	Applicable major release
Name: IK4010052 (8732) Type: equipmentAlarm Package: lte.IK4010052 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SUBUNIT 6 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RET Subunit 6 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RET Subunit 6 actuator.		

Table 29-995 IK4010053

Alarm	Attributes	Applicable major release
Name: IK4010053 (11021) Type: equipmentAlarm Package: lte.IK4010053 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: GENERAL RET FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Generic HW or SW problem of the RET device.		
Remedial action: If the alarm persists for more than a few minutes, reset the RET device. If the alarm re-appears, check whether an updated firmware is available and load it.\nIf no success, replace the RET device.		

Table 29-996 IK4011003

Alarm	Attributes	Applicable major release
Name: IK4011003 (3212) Type: equipmentAlarm Package: lte.IK4011003 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT GAIN CONTROL WARNING TX Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The RFM in Macro eNB or RFME in Metro eNB may not be able to maintain normal transmit gain on this port, but the port is still transmitting.		
Remedial action: Check the RFM (Macro) or RFME (Metro) environment. If no environmental problems are present then reset the RFM (Macro eNB) or reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then prepare for possible failure of the unit, replacement may be necessary.		

Table 29-997 IK4011004

Alarm	Attributes	Applicable major release
Name: IK4011004 (3213) Type: equipmentAlarm Package: lte.IK4011004 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT TX FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RF transmission has failed on this port.		
Remedial action: Lock and unlock cells on RFM, or further Reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then replace the RFM in Macro or the Metro Equipment."		

Table 29-998 IK4011005

Alarm	Attributes	Applicable major release
Name: IK4011005 (3214) Type: equipmentAlarm Package: lte.IK4011005 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT GAIN CONTROL TX Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM in Macro eNB or RFME in Metro eNB cannot provide the required RF gain on this port and is no longer transmitting.		
Remedial action: Reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then replace the RFM in Macro or the Metro Equipment."		

Table 29-999 IK4011006

Alarm	Attributes	Applicable major release
Name: IK4011006 (3215) Type: equipmentAlarm Package: lte.IK4011006 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT RF OUTPUT OVRDRV TX Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the RFM in Macro eNB or RFME in Metro has detected that transmit power on this port is too high so transmission for the port has been turned off. The turn off may also be caused by High reflected power: if the antenna cable is disconnected or damaged, or the antenna is damaged there may be high RF power levels reflected back into the RFM antenna port. RFMs can absorb a certain amount of this but newer high power units may not be able to absorb high return levels and so need to shut down. The power off may be also be due to High input IQ slew rates- internal slew detectors shut down the transmit path if the IQ levels swing too much for too long (5 seconds)		
Remedial action: Check for proper downlink power settings of the cells assigned to this port. Check also if the antenna cable is disconnected or damaged, or if the antenna is damaged, this may be the cause of High Reflected Power. Check also the CPRI cable connection, that may be the cause of High Input slew detectors		

Table 29-1000 IK4011007

Alarm	Attributes	Applicable major release
Name: IK4011007 (3216) Type: equipmentAlarm Package: lte.IK4011007 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT RX FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the receiver for this port has failed.		
Remedial action: Reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then replace the RFM in Macro or the Metro Equipment.		

Table 29-1001 IK4011008

Alarm	Attributes	Applicable major release
Name: IK4011008 (3217) Type: equipmentAlarm Package: lte.IK4011008 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT EQUIP FAIL TX Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the transmit amplifier for this port does not function and transmission for the port is turned off.		
Remedial action: Reset the RRH.\nAfter resetting the RRH, if the transmission continues on only one port and the same alarm is generated, check the RFM HW and replace the RFM.		

Table 29-1002 IK4011009

Alarm	Attributes	Applicable major release
Name: IK4011009 (3218) Type: equipmentAlarm Package: lte.IK4011009 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT DIGITAL INPUT OVRDRV TX Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the digital transmit signal from the modem is too high for the RFM in Macro or RFME in Metro.		
Remedial action: Reset RFM. Use the reset command on the SAM, or reset using the remote connection to NEM. If the alarm persists, contact the next level of support for a complete action plan involving, HW, SW and Eng parameters.		

Table 29-1003 IK4011010

Alarm	Attributes	Applicable major release
Name: IK4011010 (3219) Type: equipmentAlarm Package: lte.IK4011010 Raised on class: lte.AntennaPort	Severity: minor Specific problem: ANTENNA_PORT TX VSWR THRESH1 Implicitly cleared: true Default probable cause: adapterError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF transmit power reflected back into this port exceeds the warning alarm threshold.		
Remedial action: Check the cabling between Radio Module output and antenna. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If this fails to clear the alarm then replace the antenna.		

Table 29-1004 IK4011011

Alarm	Attributes	Applicable major release
Name: IK4011011 (3220) Type: equipmentAlarm Package: lte.IK4011011 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT TX VSWR THRESH2 Implicitly cleared: true Default probable cause: adapterError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF transmit power reflected back into this port exceeds the urgent alarm threshold.		
Remedial action: Check the cabling between Radio Module output and antenna. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If this fails to clear the alarm then replace the antenna		

Table 29-1005 IK4011013

Alarm	Attributes	Applicable major release
Name: IK4011013 (3222) Type: equipmentAlarm Package: lte.IK4011013 Raised on class: lte.AntennaPort	Severity: minor Specific problem: ANTENNA_PORT LNA FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the receive amplifier in the RFM or external filter module has failed.		
Remedial action: Reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then replace the RFM in Macro or the Metro Equipment or the external filter module.		

Table 29-1006 IK4011014

Alarm	Attributes	Applicable major release
Name: IK4011014 (3223) Type: equipmentAlarm Package: lte.IK4011014 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT TTLNA FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the tower-top amplifier has failed or gone into bypass.		
Remedial action: Replace the tower-top amplifier.		

Table 29-1007 IK4011015

Alarm	Attributes	Applicable major release
Name: IK4011015 (3224) Type: equipmentAlarm Package: lte.IK4011015 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This is a spare alarm. The RFM in Macro eNB or RFME in Metro eNB may not be able to maintain normal transmit gain on this port, but the port is still transmitting.		
Remedial action: Check the RFM (Macro) or RFME (Metro) environment. If no environmental problems are present then reset the RFM (Macro eNB) or reset eNB (Metro eNB) at the next maintenance window. If the alarm persists then prepare for possible failure of the unit, replacement may be necessary.		

Table 29-1008 IK4011016

Alarm	Attributes	Applicable major release
Name: IK4011016 (3225) Type: equipmentAlarm Package: lte.IK4011016 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1009 IK4011017

Alarm	Attributes	Applicable major release
Name: IK4011017 (3226) Type: equipmentAlarm Package: lte.IK4011017 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1010 IK4011018

Alarm	Attributes	Applicable major release
Name: IK4011018 (3227) Type: equipmentAlarm Package: lte.IK4011018 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1011 IK4011019

Alarm	Attributes	Applicable major release
Name: IK4011019 (3228) Type: equipmentAlarm Package: lte.IK4011019 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1012 IK4011020

Alarm	Attributes	Applicable major release
Name: IK4011020 (8733) Type: equipmentAlarm Package: lte.IK4011020 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1012 IK4011020 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1013 IK4011021

Alarm	Attributes	Applicable major release
Name: IK4011021 (8734) Type: equipmentAlarm Package: lte.IK4011021 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1014 IK4011022

Alarm	Attributes	Applicable major release
Name: IK4011022 (8735) Type: equipmentAlarm Package: lte.IK4011022 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT EVENT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Unspecified antenna port event		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1015 IK4011023

Alarm	Attributes	Applicable major release
Name: IK4011023 (10108) Type: equipmentAlarm Package: lte.IK4011023 Raised on class: lte.AntennaPort	Severity: indeterminate Specific problem: ANTENNA_PORT EVENT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Unspecified antenna port event		
Remedial action: None.		

Table 29-1016 IK4011024

Alarm	Attributes	Applicable major release
Name: IK4011024 (10109) Type: equipmentAlarm Package: lte.IK4011024 Raised on class: lte.AntennaPort	Severity: indeterminate Specific problem: ANTENNA_PORT EVENT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Unspecified antenna port event		
Remedial action: None.		

Table 29-1017 IK4011025

Alarm	Attributes	Applicable major release
Name: IK4011025 (10110) Type: equipmentAlarm Package: lte.IK4011025 Raised on class: lte.AntennaPort	Severity: warning Specific problem: ANTENNA_PORT RX PIM CANCELLATION THRESH 1 Implicitly cleared: true Default probable cause: adapterError	Release: • LR16.1.L • LR16.2.L
Description: PIM cancellation warning alarm is indication of non-linearity in the antenna system. This may be caused by damage to the RF feeders, the antenna assembly or caused from external structures. Damage may be caused by water intrusion, crimped coaxial cables, loose connectors, lightning damage, or physical damage to the antenna assembly.		
Remedial action: Check for damage to the cable between the cabling between Radio Module output and/or damage to the physical antenna assembly. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. A survey of other external PIM sources might be performed.		

Table 29-1018 IK4011026

Alarm	Attributes	Applicable major release
Name: IK4011026 (10111) Type: equipmentAlarm Package: lte.IK4011026 Raised on class: lte.AntennaPort	Severity: minor Specific problem: ANTENNA_PORT RX PIM CANCELLATION THRESH 2 Implicitly cleared: true Default probable cause: adapterError	Release: • LR16.1.L • LR16.2.L
Description: PIM cancellation minor alarm is indication of non-linearity in the antenna system. This may be caused by damage to the RF feeders, the antenna assembly or caused from external structures. Damage may be caused by water intrusion, crimped coaxial cables, loose connectors, lightning damage, or physical damage to the antenna assembly.		
Remedial action: Check for damage to the cable between the cabling between Radio Module output and/or damage to the physical antenna assembly. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. A survey of other external PIM sources might be performed.		

Table 29-1019 IK4011027

Alarm	Attributes	Applicable major release
Name: IK4011027 (10112) Type: equipmentAlarm Package: lte.IK4011027 Raised on class: lte.AntennaPort	Severity: major Specific problem: ANTENNA_PORT RX PIM CANCELLATION OUT-OF-CORRECTION RANGE Implicitly cleared: true Default probable cause: adapterError	Release: • LR16.1.L • LR16.2.L
Description: Passive Inter-Modulation (PIM) cancellation major alarm is indication that PIM Canceller is unable to remove PIM as indicated comparison of PIM power before cancellation to PIM power after cancellation. The presence of PIM is indication of non-linearity in the antenna system. This may be caused by damage to the RF feeders, the antenna assembly or caused from external structures. Damage may be caused by water intrusion, crimped coaxial cables, loose connectors, lightning damage, or physical damage to the antenna assembly.		
Remedial action: Check for damage to the cable between the cabling between Radio Module output and/or damage to the physical antenna assembly. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. A survey of other external PIM sources might be performed.		

Table 29-1020 IK4012000

Alarm	Attributes	Applicable major release
Name: IK4012000 (4023) Type: equipmentAlarm Package: lte.IK4012000 Raised on class: lte.MODULE	Severity: major Specific problem: SCB UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates failure to read manufacturer data record. Flash is available.		
Remedial action: reset if no commissioning data is available from MIM.		

Table 29-1021 IK4012001

Alarm	Attributes	Applicable major release
Name: IK4012001 (4024) Type: equipmentAlarm Package: lte.IK4012001 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB AC MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates internal Contact AC power fault.		
Remedial action: No action is required.		

Table 29-1022 IK4012002

Alarm	Attributes	Applicable major release
Name: IK4012002 (4025) Type: equipmentAlarm Package: lte.IK4012002 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB AC MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates internal Contact AC power fault.		
Remedial action: No action is required.		

Table 29-1023 IK4012003

Alarm	Attributes	Applicable major release
Name: IK4012003 (4026) Type: equipmentAlarm Package: lte.IK4012003 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB AC INPUT OUT OF SPEC Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L
Description: This alarm indicates internal Contact AC input out of specification.		
Remedial action: No action is required.		

Table 29-1024 IK4012005

Alarm	Attributes	Applicable major release
Name: IK4012005 (4028) Type: equipmentAlarm Package: lte.IK4012005 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that it fails to properly initialize represented resources.		
Remedial action: Reset.		

Table 29-1025 IK4012006

Alarm	Attributes	Applicable major release
Name: IK4012006 (4029) Type: equipmentAlarm Package: lte.IK4012006 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB OSC LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that this is a maintenance error that indicates HW failure of the OSC.		
Remedial action: Requires eNB replacement.		

Table 29-1026 IK4012007

Alarm	Attributes	Applicable major release
Name: IK4012007 (4030) Type: equipmentAlarm Package: lte.IK4012007 Raised on class: lte.MODULE	Severity: major Specific problem: SCB GPS 1PPS LOSS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the loss of 1PPS timing to timing circuitry.		
Remedial action: No action is required.		

Table 29-1027 IK4012008

Alarm	Attributes	Applicable major release
Name: IK4012008 (4031) Type: equipmentAlarm Package: lte.IK4012008 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FILE SYSTEM ACCESS FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to access files in active or passive partition.		
Remedial action: No action is required.		

Table 29-1028 IK4012009

Alarm	Attributes	Applicable major release
Name: IK4012009 (4032) Type: equipmentAlarm Package: lte.IK4012009 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB FLYWHEEL CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Flywheel (free-running) time limit reached.		
Remedial action: Reset.		

Table 29-1029 IK4012010

Alarm	Attributes	Applicable major release
Name: IK4012010 (4033) Type: equipmentAlarm Package: lte.IK4012010 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FLYWHEEL MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Flywheel (free-running) time reached major threshold.		
Remedial action: No action is required.		

Table 29-1030 IK4012011

Alarm	Attributes	Applicable major release
Name: IK4012011 (4034) Type: equipmentAlarm Package: lte.IK4012011 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FLYWHEEL MINOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Flywheel (free-running) time reached minor threshold.		
Remedial action: No action is required.		

Table 29-1031 IK4012012

Alarm	Attributes	Applicable major release
Name: IK4012012 (4035) Type: equipmentAlarm Package: lte.IK4012012 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB FLYWHEEL START Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the Flywheel (free-running) started.		
Remedial action: No action is required.		

Table 29-1032 IK4012013

Alarm	Attributes	Applicable major release
Name: IK4012013 (4036) Type: equipmentAlarm Package: lte.IK4012013 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT RAI CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the fault of CPRI port. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: Reset RFME.		

Table 29-1033 IK4012014

Alarm	Attributes	Applicable major release
Name: IK4012014 (4037) Type: equipmentAlarm Package: lte.IK4012014 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT RAI CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the fault of CPRI port. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: Reset RFME.		

Table 29-1034 IK4012019

Alarm	Attributes	Applicable major release
Name: IK4012019 (4038) Type: equipmentAlarm Package: lte.IK4012019 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT SDI CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that SAP defects indication received.		
Remedial action: No action is required.		

Table 29-1035 IK4012020

Alarm	Attributes	Applicable major release
Name: IK4012020 (4039) Type: equipmentAlarm Package: lte.IK4012020 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT SDI CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that SAP defects indication received.		
Remedial action: No action is required.		

Table 29-1036 IK4012025

Alarm	Attributes	Applicable major release
Name: IK4012025 (4040) Type: equipmentAlarm Package: lte.IK4012025 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT LOS LOF CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates loss of signal or loss of frame. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: No action is required.		

Table 29-1037 IK4012026

Alarm	Attributes	Applicable major release
Name: IK4012026 (4041) Type: equipmentAlarm Package: lte.IK4012026 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT LOS LOF CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates loss of signal or loss of frame. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: No action is required.		

Table 29-1038 IK4012030

Alarm	Attributes	Applicable major release
Name: IK4012030 (5239) Type: equipmentAlarm Package: lte.IK4012030 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates generic SW processing failure.		
Remedial action: Reset.		

Table 29-1039 IK4012031

Alarm	Attributes	Applicable major release
Name: IK4012031 (4042) Type: equipmentAlarm Package: lte.IK4012031 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB ALL CPRIPORTS FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that all CPRI ports in use are disabled due to fault condition other than missing.		
Remedial action: No action is required.		

Table 29-1040 IK4012032

Alarm	Attributes	Applicable major release
Name: IK4012032 (4043) Type: equipmentAlarm Package: lte.IK4012032 Raised on class: lte.MODULE	Severity: major Specific problem: SCB OSC OVER TEMP Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates pluggable OSM is operating at a temperature above spec limit causing performance to be degraded.		
Remedial action: No action is required.		

Table 29-1041 IK4012033

Alarm	Attributes	Applicable major release
Name: IK4012033 (4044) Type: equipmentAlarm Package: lte.IK4012033 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB SYSTEM CLOCK UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1041 IK4012033 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the system clock is not available. The alarm is applicable for 1588 system clock, syncE, GPS and external reference sources.		
Remedial action: Check the synchronization sources and provisioning.		

Table 29-1042 IK4012034

Alarm	Attributes	Applicable major release
Name: IK4012034 (4045) Type: equipmentAlarm Package: lte.IK4012034 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB LOSS OF PRIMARY REFERENCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the primary reference source is not available.		
Remedial action: Check the primary reference source.		

Table 29-1043 IK4012035

Alarm	Attributes	Applicable major release
Name: IK4012035 (4046) Type: equipmentAlarm Package: lte.IK4012035 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB LOSS OF SYNCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that Ethernet clock is insufficient to maintain 50ppb on the air interface.		
Remedial action: No action is required.		

Table 29-1044 IK4012036

Alarm	Attributes	Applicable major release
Name: IK4012036 (4047) Type: equipmentAlarm Package: lte.IK4012036 Raised on class: lte.MODULE	Severity: major Specific problem: SCB GPS ANT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates GPS Antenna failure. Set only if GPS sync source is enabled.		
Remedial action: No action is required.		

Table 29-1045 IK4012037

Alarm	Attributes	Applicable major release
Name: IK4012037 (4048) Type: equipmentAlarm Package: lte.IK4012037 Raised on class: lte.MODULE	Severity: major Specific problem: SCB GPS RECEIVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the GPS receiver has failed and cannot provide a timing reference signal.		
Remedial action: No action is required.		

Table 29-1046 IK4012038

Alarm	Attributes	Applicable major release
Name: IK4012038 (4049) Type: equipmentAlarm Package: lte.IK4012038 Raised on class: lte.MODULE	Severity: major Specific problem: SCB GPS RECEIVER COMM FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the GPS receiver communication failure.		
Remedial action: No action is required.		

Table 29-1047 IK4012039

Alarm	Attributes	Applicable major release
Name: IK4012039 (4050) Type: equipmentAlarm Package: lte.IK4012039 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB GPS ANT POSITION UNKNOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates GPS antenna position unknown. Set only if Geo-Based location service required.		
Remedial action: Check the position of the GPS antenna.		

Table 29-1048 IK4012040

Alarm	Attributes	Applicable major release
Name: IK4012040 (4051) Type: equipmentAlarm Package: lte.IK4012040 Raised on class: lte.MODULE	Severity: major Specific problem: SCB OVER TEMP MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the CCM temperature is rising near the shutdown limit.		
Remedial action: No action is required.		

Table 29-1049 IK4012041

Alarm	Attributes	Applicable major release
Name: IK4012041 (4052) Type: equipmentAlarm Package: lte.IK4012041 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB OVER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the CCM temperature is above operating range.		
Remedial action: Board will autonomously power down.		

Table 29-1050 IK4012042

Alarm	Attributes	Applicable major release
Name: IK4012042 (4053) Type: equipmentAlarm Package: lte.IK4012042 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB PTP LOSS OF PRIMARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates indicate the lack of SYNCH message from the primary server when SYNCH messages have not been received for the period set by the SYNCH_RECEIPT_TIMEOUT_EXPIRES event in the client .		
Remedial action: No action is required.		

Table 29-1051 IK4012043

Alarm	Attributes	Applicable major release
Name: IK4012043 (4054) Type: equipmentAlarm Package: lte.IK4012043 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB PTP LOSS OF SECONDARY SYNCHRONIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates indicate the lack of SYNCH message from the secondary server when SYNCH messages have not been received for the period set by the SYNCH_RECEIPT_TIMEOUT_EXPIRES event in the client .		
Remedial action: No action is required.		

Table 29-1052 IK4012044

Alarm	Attributes	Applicable major release
Name: IK4012044 (4055) Type: equipmentAlarm Package: lte.IK4012044 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB UNEXPECTED LONG INITIALIZATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that PTP engine has taken longer than expected to achieve complete synchronization.		
Remedial action: No action is required.		

Table 29-1053 IK4012045

Alarm	Attributes	Applicable major release
Name: IK4012045 (4056) Type: equipmentAlarm Package: lte.IK4012045 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB PTP CLIENT INITIALIZING 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the alarm is active on cold-start when the primary Grandmaster server is in the initializing state.		
Remedial action: No action is required.		

Table 29-1054 IK4012046

Alarm	Attributes	Applicable major release
Name: IK4012046 (4057) Type: equipmentAlarm Package: lte.IK4012046 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB PTP CLIENT INITIALIZING 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the alarm is active on cold-start when the secondary Grandmaster server is in the initializing state.		
Remedial action: No action is required.		

Table 29-1055 IK4012047

Alarm	Attributes	Applicable major release
Name: IK4012047 (4058) Type: equipmentAlarm Package: lte.IK4012047 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB GPS LOCK FAILURE CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1055 IK4012047 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that GPS is not locked.		
Remedial action: No action is required.		

Table 29-1056 IK4012048

Alarm	Attributes	Applicable major release
Name: IK4012048 (4059) Type: equipmentAlarm Package: lte.IK4012048 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LOOPBACK INACTIVITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates there is no packet activity for the interval specified in the loopback activation.		
Remedial action: No action is required.		

Table 29-1057 IK4012051

Alarm	Attributes	Applicable major release
Name: IK4012051 (4062) Type: equipmentAlarm Package: lte.IK4012051 Raised on class: lte.MODULE	Severity: major Specific problem: SCB GPS INSUFFICIENT FIXED SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the available fixed satellites are less than the required ones to get GPS synchronization. The alarm will only be generated when GPS is configured as the synchronization source.		
Remedial action: No action is required.		

Table 29-1058 IK4012052

Alarm	Attributes	Applicable major release
Name: IK4012052 (4063) Type: equipmentAlarm Package: lte.IK4012052 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 1 SOFTWARE WARNING 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 1 software warning.		
Remedial action: No action is required.		

Table 29-1059 IK4012053

Alarm	Attributes	Applicable major release
Name: IK4012053 (4064) Type: equipmentAlarm Package: lte.IK4012053 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 1 SOFTWARE WARNING 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 1 software warning.		
Remedial action: No action is required.		

Table 29-1060 IK4012054

Alarm	Attributes	Applicable major release
Name: IK4012054 (4065) Type: equipmentAlarm Package: lte.IK4012054 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 1 SOFTWARE WARNING 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 1 software warning.		
Remedial action: No action is required.		

Table 29-1061 IK4012055

Alarm	Attributes	Applicable major release
Name: IK4012055 (4066) Type: equipmentAlarm Package: lte.IK4012055 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 2 SOFTWARE WARNING 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 2 software warning.		
Remedial action: No action is required.		

Table 29-1062 IK4012056

Alarm	Attributes	Applicable major release
Name: IK4012056 (4067) Type: equipmentAlarm Package: lte.IK4012056 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 2 SOFTWARE WARNING 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-1062 IK4012056 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a Layer 2 software warning.		
Remedial action: No action is required.		

Table 29-1063 IK4012057

Alarm	Attributes	Applicable major release
Name: IK4012057 (4068) Type: equipmentAlarm Package: lte.IK4012057 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB LAYER 2 SOFTWARE WARNING 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a Layer 2 software warning.		
Remedial action: No action is required.		

Table 29-1064 IK4012058

Alarm	Attributes	Applicable major release
Name: IK4012058 (4069) Type: equipmentAlarm Package: lte.IK4012058 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB LED FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to control face-plate LEDs.		
Remedial action: No action is required.		

Table 29-1065 IK4012062

Alarm	Attributes	Applicable major release
Name: IK4012062 (4073) Type: equipmentAlarm Package: lte.IK4012062 Raised on class: lte.MODULE	Severity: minor Specific problem: METRO BOX DOOR ALARM Implicitly cleared: true Default probable cause: enclosureDoorOpen	Release: • LR15.1.L
Description: This alarm indicates that the Metro box was opened.		
Remedial action: No action is required.		

Table 29-1066 IK4012063

Alarm	Attributes	Applicable major release
Name: IK4012063 (4074) Type: equipmentAlarm Package: lte.IK4012063 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified SCB fault detected		
Remedial action: No action is required.		

Table 29-1067 IK4012064

Alarm	Attributes	Applicable major release
Name: IK4012064 (4075) Type: equipmentAlarm Package: lte.IK4012064 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified SCB fault detected		
Remedial action: No action is required.		

Table 29-1068 IK4012065

Alarm	Attributes	Applicable major release
Name: IK4012065 (4076) Type: equipmentAlarm Package: lte.IK4012065 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SCB fault detected		
Remedial action: No action is required.		

Table 29-1069 IK4012066

Alarm	Attributes	Applicable major release
Name: IK4012066 (4077) Type: equipmentAlarm Package: lte.IK4012066 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SCB fault detected		

Table 29-1069 IK4012066 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1070 IK4012067

Alarm	Attributes	Applicable major release
Name: IK4012067 (4078) Type: equipmentAlarm Package: lte.IK4012067 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SCB fault detected		
Remedial action: No action is required.		

Table 29-1071 IK4012068

Alarm	Attributes	Applicable major release
Name: IK4012068 (4691) Type: equipmentAlarm Package: lte.IK4012068 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB GPS LOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that GPS satellite lock has been lost after timing has been synchronized.		
Remedial action: Check the GPS antenna placement, GPS antenna status, or GPS antenna cable. Replace the External GPS Receiver or SCB (if using internal GPS receiver).		

Table 29-1072 IK4012069

Alarm	Attributes	Applicable major release
Name: IK4012069 (4692) Type: equipmentAlarm Package: lte.IK4012069 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB GPS INSUFFICIENT VISIBLE SATELLITES Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that insufficient visible satellites are available to get GPS synchronization.		
Remedial action: Check the GPS antenna location and status. Replace GPS antenna, cable or receiver if necessary.		

Table 29-1073 IK4012070

Alarm	Attributes	Applicable major release
Name: IK4012070 (4693) Type: processingErrorAlarm Package: lte.IK4012070 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L1 SOFTWARE FAIL SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1074 IK4012071

Alarm	Attributes	Applicable major release
Name: IK4012071 (4694) Type: processingErrorAlarm Package: lte.IK4012071 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L1 SOFTWARE FAIL SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1075 IK4012072

Alarm	Attributes	Applicable major release
Name: IK4012072 (4695) Type: processingErrorAlarm Package: lte.IK4012072 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L1 SOFTWARE FAIL SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1076 IK4012073

Alarm	Attributes	Applicable major release
Name: IK4012073 (4696) Type: equipmentAlarm Package: lte.IK4012073 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB L1 HARDWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware failure.		
Remedial action: Reset the Modem Function, replace the eNodeB if the problem persists.		

Table 29-1077 IK4012074

Alarm	Attributes	Applicable major release
Name: IK4012074 (4697) Type: processingErrorAlarm Package: lte.IK4012074 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L2 SOFTWARE FAIL SLICE 1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1078 IK4012075

Alarm	Attributes	Applicable major release
Name: IK4012075 (4698) Type: processingErrorAlarm Package: lte.IK4012075 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L2 SOFTWARE FAIL SLICE 2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1079 IK4012076

Alarm	Attributes	Applicable major release
Name: IK4012076 (4699) Type: processingErrorAlarm Package: lte.IK4012076 Raised on class: lte.MODULE	Severity: major Specific problem: SCB L2 SOFTWARE FAIL SLICE 3 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on the Modem Function.		
Remedial action: Reset the modem.		

Table 29-1080 IK4012077

Alarm	Attributes	Applicable major release
Name: IK4012077 (4700) Type: equipmentAlarm Package: lte.IK4012077 Raised on class: lte.MODULE	Severity: major Specific problem: BTS PACKAGE TYPE NOT RECOGNIZED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the BTS package type is not recognized.		
Remedial action: Re-configure to correct BTS package type.		

Table 29-1081 IK4012078

Alarm	Attributes	Applicable major release
Name: IK4012078 (7991) Type: equipmentAlarm Package: lte.IK4012078 Raised on class: lte.MODULE	Severity: warning Specific problem: SCB INIT GPS SELF SURVEY FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that high accuracy GPS self survey for OTDOA sync has not been successfully completed after 24 hours.		
Remedial action: Check GPS performance. Ensure good GPS receiver and GPS antenna is installed per Nokia guidelines and located to have a full sky visibility with no local interference or multipath, then power cycle the controller to restart survey. If GPS reception can't be improved then disable OTDOA sync (isGeoLocPhaseSyncAllowed="False), which will clear the alarm."		

Table 29-1082 IK4012079

Alarm	Attributes	Applicable major release
Name: IK4012079 (7992) Type: equipmentAlarm Package: lte.IK4012079 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB INIT GPS SELF SURVEY INPROGRESS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This event indicates that the eNB has started a high accuracy GPS survey for OTDOA, which normally takes 10 hours to complete.		
Remedial action: No action is required.		

Table 29-1083 IK4012087

Alarm	Attributes	Applicable major release
Name: IK4012087 (8736) Type: equipmentAlarm Package: lte.IK4012087 Raised on classes: • lte.BBCardSpecifics • lte.MODULE	Severity: minor Specific problem: LED FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to control face-plate LEDs.		
Remedial action: Reset the system in low traffic hours		

Table 29-1084 IK4012090

Alarm	Attributes	Applicable major release
Name: IK4012090 (8737) Type: equipmentAlarm Package: lte.IK4012090 Raised on class: lte.MODULE	Severity: critical Specific problem: SCB CASW LOSS OF SIGNAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Alarm indicates the Loss Of Signal at the CASW (AD8155) receiver		
Remedial action: Disable Carrier Aggregation/Dual Carrier metro features		

Table 29-1085 IK4012092

Alarm	Attributes	Applicable major release
Name: IK4012092 (10113) Type: equipmentAlarm Package: lte.IK4012092 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: GNSS MODE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNB does not support Glonass or GPS+Glonass mode. It only supports GPS mode		
Remedial action: Change the configuration of the eNB by configuring the GPS mode.		

Table 29-1086 IK4012095

Alarm	Attributes	Applicable major release
Name: IK4012095 (11022) Type: equipmentAlarm Package: lte.IK4012095 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT RAI INTERNAL CPRI Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the fault of CPRI port. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: Reset RFME.		

Table 29-1087 IK4012096

Alarm	Attributes	Applicable major release
Name: IK4012096 (11023) Type: equipmentAlarm Package: lte.IK4012096 Raised on class: lte.MODULE	Severity: minor Specific problem: SCB FAULT SDI INTERNAL CPRI Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1087 IK4012096 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that SAP defects indication received.		
Remedial action: No action is required.		

Table 29-1088 IK4012097

Alarm	Attributes	Applicable major release
Name: IK4012097 (11024) Type: equipmentAlarm Package: lte.IK4012097 Raised on class: lte.MODULE	Severity: major Specific problem: SCB FAULT LOS LOF INTERNAL CPRI Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates loss of signal or loss of frame. Change the K_IET_CMPLX_CPRI_STATE_n to (disable/failed/NA).		
Remedial action: No action is required.		

Table 29-1089 IK4012098

Alarm	Attributes	Applicable major release
Name: IK4012098 (11025) Type: equipmentAlarm Package: lte.IK4012098 Raised on class: lte.MODULE	Severity: minor Specific problem: CR NOT PRESENT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: It indicates Clock Recovery Module (Support for the SYNCE function) is not present. Synce function could not work.		
Remedial action: To check the HW whether there is such module mounted in the Dock.\nTo check whether the SYNCE related function is needed/expected.		

Table 29-1090 IK4013000

Alarm	Attributes	Applicable major release
Name: IK4013000 (4079) Type: equipmentAlarm Package: lte.IK4013000 Raised on class: lte.RFME	Severity: critical Specific problem: RFME COMM FAIL Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L
Description: This alarm indicates the loss of RFME communication.		
Remedial action: No action is required.		

Table 29-1091 IK4013001

Alarm	Attributes	Applicable major release
Name: IK4013001 (4080) Type: equipmentAlarm Package: lte.IK4013001 Raised on class: lte.RFME	Severity: minor Specific problem: RFME UNDER TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFME ambient temperature is low.		
Remedial action: No action is required.		

Table 29-1092 IK4013002

Alarm	Attributes	Applicable major release
Name: IK4013002 (4081) Type: equipmentAlarm Package: lte.IK4013002 Raised on class: lte.RFME	Severity: critical Specific problem: RFME WARM UP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFME ambient temperature is too low.		
Remedial action: Wait.		

Table 29-1093 IK4013003

Alarm	Attributes	Applicable major release
Name: IK4013003 (4082) Type: equipmentAlarm Package: lte.IK4013003 Raised on class: lte.RFME	Severity: minor Specific problem: RFME OVER TEMP WARNING Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L
Description: This alarm indicates that the RFME ambient temperature is high.		
Remedial action: No action is required.		

Table 29-1094 IK4013004

Alarm	Attributes	Applicable major release
Name: IK4013004 (4083) Type: equipmentAlarm Package: lte.IK4013004 Raised on class: lte.RFME	Severity: critical Specific problem: RFME CRITICAL TEMP Implicitly cleared: true Default probable cause: heatingOrVentilationOrCoolingSystemProblem	Release: • LR15.1.L

Table 29-1094 IK4013004 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RFME temperature is high.		
Remedial action: Disable.		

Table 29-1095 IK4013005

Alarm	Attributes	Applicable major release
Name: IK4013005 (4084) Type: equipmentAlarm Package: lte.IK4013005 Raised on class: lte.RFME	Severity: critical Specific problem: RFME ST CRITICAL FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the RFME Hardware failure.		
Remedial action: Init.		

Table 29-1096 IK4013006

Alarm	Attributes	Applicable major release
Name: IK4013006 (4085) Type: equipmentAlarm Package: lte.IK4013006 Raised on class: lte.RFME	Severity: critical Specific problem: RFME INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the RFME initialization failure.		
Remedial action: Init.		

Table 29-1097 IK4013008

Alarm	Attributes	Applicable major release
Name: IK4013008 (4087) Type: equipmentAlarm Package: lte.IK4013008 Raised on class: lte.RFME	Severity: major Specific problem: RFME SIGNAL QUALITY Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the RFME signal quality.		
Remedial action: No action is required.		

Table 29-1098 IK4013009

Alarm	Attributes	Applicable major release
Name: IK4013009 (4088) Type: equipmentAlarm Package: lte.IK4013009 Raised on class: lte.RFME	Severity: major Specific problem: RFME INPUT VOLTAGE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the input voltage is very high or very low.		
Remedial action: No action is required.		

Table 29-1099 IK4013010

Alarm	Attributes	Applicable major release
Name: IK4013010 (4089) Type: equipmentAlarm Package: lte.IK4013010 Raised on class: lte.RFME	Severity: critical Specific problem: RFME PWR CONVERTER FAIL Implicitly cleared: true Default probable cause: powerProblem	Release: • LR15.1.L
Description: The RFME internal power converter has failed.		
Remedial action: Init.		

Table 29-1100 IK4013011

Alarm	Attributes	Applicable major release
Name: IK4013011 (4090) Type: equipmentAlarm Package: lte.IK4013011 Raised on class: lte.RFME	Severity: critical Specific problem: RFME CLOCK FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The RFME cannot derive proper clock signal from the incoming CPRI link.		
Remedial action: Init		

Table 29-1101 IK4013012

Alarm	Attributes	Applicable major release
Name: IK4013012 (4091) Type: equipmentAlarm Package: lte.IK4013012 Raised on class: lte.RFME	Severity: critical Specific problem: RFME RF SYNTH FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The RFME internal frequency synthesizer is out of lock.		
Remedial action: Init.		

Table 29-1102 IK4013015

Alarm	Attributes	Applicable major release
Name: IK4013015 (4092) Type: equipmentAlarm Package: lte.IK4013015 Raised on class: lte.RFME	Severity: warning Specific problem: RFME UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to read the manufacturer data.		
Remedial action: Init		

Table 29-1103 IK4013017

Alarm	Attributes	Applicable major release
Name: IK4013017 (4094) Type: equipmentAlarm Package: lte.IK4013017 Raised on class: lte.RFME	Severity: major Specific problem: RFME BIST PARTIAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that at least one failure was detected during power on self-test, but the unit may still be functional, though in a degraded state.		
Remedial action: No action is required.		

Table 29-1104 IK4013018

Alarm	Attributes	Applicable major release
Name: IK4013018 (4095) Type: equipmentAlarm Package: lte.IK4013018 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOF PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that framing cannot be recovered at the slave link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1105 IK4013019

Alarm	Attributes	Applicable major release
Name: IK4013019 (4096) Type: equipmentAlarm Package: lte.IK4013019 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOF PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L

Table 29-1105 IK4013019 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that framing cannot be recovered at the slave link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1106 IK4013020

Alarm	Attributes	Applicable major release
Name: IK4013020 (4097) Type: equipmentAlarm Package: lte.IK4013020 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOF PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that framing cannot be recovered at the slave link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1107 IK4013021

Alarm	Attributes	Applicable major release
Name: IK4013021 (4098) Type: equipmentAlarm Package: lte.IK4013021 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOS PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1108 IK4013022

Alarm	Attributes	Applicable major release
Name: IK4013022 (4099) Type: equipmentAlarm Package: lte.IK4013022 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOS PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1109 IK4013023

Alarm	Attributes	Applicable major release
Name: IK4013023 (4100) Type: equipmentAlarm Package: lte.IK4013023 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK LOS PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that no signal is detected at the link port. This alarm is enabled only after the link is established.		
Remedial action: No action is required.		

Table 29-1110 IK4013024

Alarm	Attributes	Applicable major release
Name: IK4013024 (4101) Type: equipmentAlarm Package: lte.IK4013024 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK RAI PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: No action is required.		

Table 29-1111 IK4013025

Alarm	Attributes	Applicable major release
Name: IK4013025 (4102) Type: equipmentAlarm Package: lte.IK4013025 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK RAI PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: No action is required.		

Table 29-1112 IK4013026

Alarm	Attributes	Applicable major release
Name: IK4013026 (4103) Type: equipmentAlarm Package: lte.IK4013026 Raised on class: lte.RFME	Severity: major Specific problem: RFME LINK RAI PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming slave link RAI bit is set.		
Remedial action: No action is required.		

Table 29-1113 IK4013027

Alarm	Attributes	Applicable major release
Name: IK4013027 (4104) Type: equipmentAlarm Package: lte.IK4013027 Raised on class: lte.RFME	Severity: minor Specific problem: RFME SIGNAL LOW PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: No action is required.		

Table 29-1114 IK4013028

Alarm	Attributes	Applicable major release
Name: IK4013028 (4105) Type: equipmentAlarm Package: lte.IK4013028 Raised on class: lte.RFME	Severity: minor Specific problem: RFME SIGNAL LOW PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: No action is required.		

Table 29-1115 IK4013029

Alarm	Attributes	Applicable major release
Name: IK4013029 (4106) Type: equipmentAlarm Package: lte.IK4013029 Raised on class: lte.RFME	Severity: minor Specific problem: RFME SIGNAL LOW PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the optical signal strength is very low on the slave link port.		
Remedial action: No action is required.		

Table 29-1116 IK4013030

Alarm	Attributes	Applicable major release
Name: IK4013030 (4107) Type: equipmentAlarm Package: lte.IK4013030 Raised on class: lte.RFME	Severity: minor Specific problem: RFME BER PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: No action is required.		

Table 29-1117 IK4013031

Alarm	Attributes	Applicable major release
Name: IK4013031 (4108) Type: equipmentAlarm Package: lte.IK4013031 Raised on class: lte.RFME	Severity: minor Specific problem: RFME BER PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: No action is required.		

Table 29-1118 IK4013032

Alarm	Attributes	Applicable major release
Name: IK4013032 (4109) Type: equipmentAlarm Package: lte.IK4013032 Raised on class: lte.RFME	Severity: minor Specific problem: RFME BER PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates excessive bit errors on the CPRI link.		
Remedial action: No action is required.		

Table 29-1119 IK4013033

Alarm	Attributes	Applicable major release
Name: IK4013033 (4110) Type: equipmentAlarm Package: lte.IK4013033 Raised on class: lte.RFME	Severity: major Specific problem: RFME SIGNAL SDI PORT1 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: No action is required.		

Table 29-1120 IK4013034

Alarm	Attributes	Applicable major release
Name: IK4013034 (4111) Type: equipmentAlarm Package: lte.IK4013034 Raised on class: lte.RFME	Severity: major Specific problem: RFME SIGNAL SDI PORT2 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: No action is required.		

Table 29-1121 IK4013035

Alarm	Attributes	Applicable major release
Name: IK4013035 (4112) Type: equipmentAlarm Package: lte.IK4013035 Raised on class: lte.RFME	Severity: major Specific problem: RFME SIGNAL SDI PORT3 Implicitly cleared: true Default probable cause: inputDeviceError	Release: • LR15.1.L
Description: This alarm indicates that the incoming CPRI link SDI bit is set.		
Remedial action: No action is required.		

Table 29-1122 IK4013036

Alarm	Attributes	Applicable major release
Name: IK4013036 (4113) Type: equipmentAlarm Package: lte.IK4013036 Raised on class: lte.RFME	Severity: minor Specific problem: RFME MESSAGE THROTTLING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the RF is generating too many messages over the CPRI link.		
Remedial action: No action is required.		

Table 29-1123 IK4013038

Alarm	Attributes	Applicable major release
Name: IK4013038 (4115) Type: equipmentAlarm Package: lte.IK4013038 Raised on class: lte.RFME	Severity: minor Specific problem: RFME FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		
Remedial action: No action is required.		

Table 29-1124 IK4013039

Alarm	Attributes	Applicable major release
Name: IK4013039 (4116) Type: equipmentAlarm Package: lte.IK4013039 Raised on class: lte.RFME	Severity: minor Specific problem: RFME FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		

Table 29-1124 IK4013039 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1125 IK4013040

Alarm	Attributes	Applicable major release
Name: IK4013040 (4117) Type: equipmentAlarm Package: lte.IK4013040 Raised on class: lte.RFME	Severity: minor Specific problem: RFME FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		
Remedial action: No action is required.		

Table 29-1126 IK4013041

Alarm	Attributes	Applicable major release
Name: IK4013041 (4118) Type: equipmentAlarm Package: lte.IK4013041 Raised on class: lte.RFME	Severity: minor Specific problem: RFME FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		
Remedial action: No action is required.		

Table 29-1127 IK4013046

Alarm	Attributes	Applicable major release
Name: IK4013046 (8738) Type: equipmentAlarm Package: lte.IK4013046 Raised on class: lte.RFME	Severity: minor Specific problem: RFME NOT ALLOWED BY ENB TYPE LICENSE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the licence for the eNB type does not allow this RFME. The performance of this RFME goes beyond what the licence for the eNB type allows		
Remedial action: No action is required. The operator has to use another and appropriate RFME.		

Table 29-1128 IK4013047

Alarm	Attributes	Applicable major release
Name: IK4013047 (8739) Type: equipmentAlarm Package: lte.IK4013047 Raised on class: lte.RFME	Severity: minor Specific problem: RFME FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		
Remedial action: No action is required.		

Table 29-1129 IK4013048

Alarm	Attributes	Applicable major release
Name: IK4013048 (8740) Type: equipmentAlarm Package: lte.IK4013048 Raised on class: lte.RFME	Severity: major Specific problem: RFME FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RFME fault detected		
Remedial action: No action is required.		

Table 29-1130 IK4013054

Alarm	Attributes	Applicable major release
Name: IK4013054 (8741) Type: equipmentAlarm Package: lte.IK4013054 Raised on class: lte.RFME	Severity: critical Specific problem: RFME FAULT DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software download failure.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support. required.		

Table 29-1131 IK4014001

Alarm	Attributes	Applicable major release
Name: IK4014001 (4701) Type: equipmentAlarm Package: lte.IK4014001 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: MEDO DETECTION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1131 IK4014001 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure to detect the presence of MEDO.		
Remedial action: Call the next level of support.		

Table 29-1132 IK4014003

Alarm	Attributes	Applicable major release
Name: IK4014003 (4703) Type: equipmentAlarm Package: lte.IK4014003 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO UNREADABLE MANUFACTURER DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to read the manufacturer data.		
Remedial action: Call the next level of support.		

Table 29-1133 IK4014009

Alarm	Attributes	Applicable major release
Name: IK4014009 (4998) Type: equipmentAlarm Package: lte.IK4014009 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO MEMORY ACCESS FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to access the EEPROM on the Metro Dock		
Remedial action: Call the next level of support.		

Table 29-1134 IK4014010

Alarm	Attributes	Applicable major release
Name: IK4014010 (8742) Type: equipmentAlarm Package: lte.IK4014010 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: POWER OVER ETHERNET CONNECTION FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: PoE Power Turned off due to problem with Powered Device or connection to Powered Device.		
Remedial action: Check Powered Device and Ethernet cable for faults, and take necessary repair steps.		

Table 29-1135 IK4014011

Alarm	Attributes	Applicable major release
Name: IK4014011 (8743) Type: equipmentAlarm Package: lte.IK4014011 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: POWER OVER ETHERNET HW FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The Power over Ethernet hardware has a failure and is not able to supply power to a Powered Device.		
Remedial action: If the Additional Information indicates Thermal Shutdown, check the ambient temperature of the eNB. Otherwise, if the failure persists, and if Power over Ethernet support is needed, the backhaul module of the eNB should be replaced.		

Table 29-1136 IK4014012

Alarm	Attributes	Applicable major release
Name: IK4014012 (8744) Type: equipmentAlarm Package: lte.IK4014012 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: POWERED DEVICE ATTACHED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The Power over Ethernet hardware has detected that a valid Powered Device has attached to the eNB.		
Remedial action: None		

Table 29-1137 IK4014013

Alarm	Attributes	Applicable major release
Name: IK4014013 (8745) Type: equipmentAlarm Package: lte.IK4014013 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: POWERED DEVICE DETACHED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The Power over Ethernet hardware has detected that a valid Powered Device has detached from the eNB.		
Remedial action: None		

Table 29-1138 IK4014014

Alarm	Attributes	Applicable major release
Name: IK4014014 (8746) Type: equipmentAlarm Package: lte.IK4014014 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1138 IK4014014 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare event for MEDO for future use.		
Remedial action: No action is required.		

Table 29-1139 IK4014015

Alarm	Attributes	Applicable major release
Name: IK4014015 (8747) Type: equipmentAlarm Package: lte.IK4014015 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO EVENT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for MEDO for future use.		
Remedial action: No action is required.		

Table 29-1140 IK4014016

Alarm	Attributes	Applicable major release
Name: IK4014016 (8748) Type: equipmentAlarm Package: lte.IK4014016 Raised on class: lte.ENBEquipment	Severity: major Specific problem: MEDO FAULT 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1141 IK4014017

Alarm	Attributes	Applicable major release
Name: IK4014017 (8749) Type: equipmentAlarm Package: lte.IK4014017 Raised on class: lte.ENBEquipment	Severity: major Specific problem: MEDO FAULT 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1142 IK4014018

Alarm	Attributes	Applicable major release
Name: IK4014018 (10114) Type: equipmentAlarm Package: lte.IK4014018 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO HRAL FAULT 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1143 IK4014019

Alarm	Attributes	Applicable major release
Name: IK4014019 (10115) Type: equipmentAlarm Package: lte.IK4014019 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO HRAL EVENT 6 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for MEDO for future use.		
Remedial action: None.		

Table 29-1144 IK4015000

Alarm	Attributes	Applicable major release
Name: IK4015000 (5240) Type: equipmentAlarm Package: lte.IK4015000 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB FAILURE SLAVE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of a Slave SOC.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. Replace the BB If the problem persists.		

Table 29-1145 IK4015001

Alarm	Attributes	Applicable major release
Name: IK4015001 (5241) Type: equipmentAlarm Package: lte.IK4015001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB FAILURE SLAVE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of a Slave SOC.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. Replace the BB If the problem persists.		

Table 29-1146 IK4015002

Alarm	Attributes	Applicable major release
Name: IK4015002 (5242) Type: equipmentAlarm Package: lte.IK4015002 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB CARD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure of modem board.		
Remedial action: The modem board is automatically reset to attempt to clear the fault.Replace the BB If the problem persists.		

Table 29-1147 IK4015007

Alarm	Attributes	Applicable major release
Name: IK4015007 (5243) Type: equipmentAlarm Package: lte.IK4015007 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1148 IK4015008

Alarm	Attributes	Applicable major release
Name: IK4015008 (5244) Type: equipmentAlarm Package: lte.IK4015008 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1149 IK4015009

Alarm	Attributes	Applicable major release
Name: IK4015009 (5245) Type: equipmentAlarm Package: lte.IK4015009 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1150 IK4015010

Alarm	Attributes	Applicable major release
Name: IK4015010 (5246) Type: equipmentAlarm Package: lte.IK4015010 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1151 IK4015011

Alarm	Attributes	Applicable major release
Name: IK4015011 (5247) Type: equipmentAlarm Package: lte.IK4015011 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1152 IK4015012

Alarm	Attributes	Applicable major release
Name: IK4015012 (5248) Type: equipmentAlarm Package: lte.IK4015012 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS LSL CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The incoming optical signal level for this CPRI port is very low.		
Remedial action: Check the CPRI link connections, cables, and SFPs and replace as necessary.		

Table 29-1153 IK4015013

Alarm	Attributes	Applicable major release
Name: IK4015013 (5249) Type: equipmentAlarm Package: lte.IK4015013 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1154 IK4015014

Alarm	Attributes	Applicable major release
Name: IK4015014 (5250) Type: equipmentAlarm Package: lte.IK4015014 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1155 IK4015015

Alarm	Attributes	Applicable major release
Name: IK4015015 (5251) Type: equipmentAlarm Package: lte.IK4015015 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1156 IK4015016

Alarm	Attributes	Applicable major release
Name: IK4015016 (5252) Type: equipmentAlarm Package: lte.IK4015016 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1157 IK4015017

Alarm	Attributes	Applicable major release
Name: IK4015017 (5253) Type: equipmentAlarm Package: lte.IK4015017 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1158 IK4015018

Alarm	Attributes	Applicable major release
Name: IK4015018 (5254) Type: equipmentAlarm Package: lte.IK4015018 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB LOS LOF CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the CPRI link from the first RFM on this port has failed (Loss of signal and/or loss of framing)		
Remedial action: Check the CPRI link cable and SFPs (BB and RFM) for failures, otherwise reset the RFM or reset the BB		

Table 29-1159 IK4015019

Alarm	Attributes	Applicable major release
Name: IK4015019 (5255) Type: equipmentAlarm Package: lte.IK4015019 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1160 IK4015020

Alarm	Attributes	Applicable major release
Name: IK4015020 (5256) Type: equipmentAlarm Package: lte.IK4015020 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1161 IK4015021

Alarm	Attributes	Applicable major release
Name: IK4015021 (5257) Type: equipmentAlarm Package: lte.IK4015021 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1161 IK4015021 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1162 IK4015022

Alarm	Attributes	Applicable major release
Name: IK4015022 (5258) Type: equipmentAlarm Package: lte.IK4015022 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1163 IK4015023

Alarm	Attributes	Applicable major release
Name: IK4015023 (5259) Type: equipmentAlarm Package: lte.IK4015023 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1164 IK4015024

Alarm	Attributes	Applicable major release
Name: IK4015024 (5260) Type: equipmentAlarm Package: lte.IK4015024 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB TRANS TX FAILURE CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure in the BB CPRI port transmitter.		
Remedial action: Replace the SFP for this port.		

Table 29-1165 IK4015025

Alarm	Attributes	Applicable major release
Name: IK4015025 (5261) Type: equipmentAlarm Package: lte.IK4015025 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1166 IK4015026

Alarm	Attributes	Applicable major release
Name: IK4015026 (5262) Type: equipmentAlarm Package: lte.IK4015026 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1167 IK4015027

Alarm	Attributes	Applicable major release
Name: IK4015027 (5263) Type: equipmentAlarm Package: lte.IK4015027 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1168 IK4015028

Alarm	Attributes	Applicable major release
Name: IK4015028 (5264) Type: equipmentAlarm Package: lte.IK4015028 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1169 IK4015029

Alarm	Attributes	Applicable major release
Name: IK4015029 (5265) Type: equipmentAlarm Package: lte.IK4015029 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1170 IK4015030

Alarm	Attributes	Applicable major release
Name: IK4015030 (5266) Type: equipmentAlarm Package: lte.IK4015030 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB TRANS RX LOS CPRIPORT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: No CPRI signal is received at this CPRI port.		
Remedial action: Check the CPRI cable and connections, replace the SFP (RFM or BB end), verify the RFM is operating.		

Table 29-1171 IK4015031

Alarm	Attributes	Applicable major release
Name: IK4015031 (5267) Type: equipmentAlarm Package: lte.IK4015031 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB ALL CPRIPORTS FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of all CPRI ports.		
Remedial action: Replace the BB if the problem persists		

Table 29-1172 IK4016000

Alarm	Attributes	Applicable major release
Name: IK4016000 (5268) Type: equipmentAlarm Package: lte.IK4016000 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INDETERMINATE OPERATIONAL FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a modem board has been detected that cannot described by any specific alarm.		

Table 29-1172 IK4016000 (continued)

Alarm	Attributes	Applicable major release
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1173 IK4016001

Alarm	Attributes	Applicable major release
Name: IK4016001 (5269) Type: equipmentAlarm Package: lte.IK4016001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INIT FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize a SOC of a modem board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1174 IK4016002

Alarm	Attributes	Applicable major release
Name: IK4016002 (5270) Type: equipmentAlarm Package: lte.IK4016002 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB L1 HARDWARE FAIL SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1175 IK4016003

Alarm	Attributes	Applicable major release
Name: IK4016003 (5271) Type: processingErrorAlarm Package: lte.IK4016003 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1176 IK4016004

Alarm	Attributes	Applicable major release
Name: IK4016004 (5272) Type: processingErrorAlarm Package: lte.IK4016004 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1177 IK4016005

Alarm	Attributes	Applicable major release
Name: IK4016005 (5273) Type: processingErrorAlarm Package: lte.IK4016005 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1178 IK4016006

Alarm	Attributes	Applicable major release
Name: IK4016006 (5274) Type: processingErrorAlarm Package: lte.IK4016006 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1179 IK4016007

Alarm	Attributes	Applicable major release
Name: IK4016007 (5275) Type: equipmentAlarm Package: lte.IK4016007 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB MODEM CELL RESOURCES FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1179 IK4016007 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1180 IK4016008

Alarm	Attributes	Applicable major release
Name: IK4016008 (5276) Type: processingErrorAlarm Package: lte.IK4016008 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1181 IK4016009

Alarm	Attributes	Applicable major release
Name: IK4016009 (5277) Type: processingErrorAlarm Package: lte.IK4016009 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1182 IK4016010

Alarm	Attributes	Applicable major release
Name: IK4016010 (5278) Type: equipmentAlarm Package: lte.IK4016010 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 1 SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1183 IK4016011

Alarm	Attributes	Applicable major release
Name: IK4016011 (5279) Type: equipmentAlarm Package: lte.IK4016011 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 2 SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1184 IK4017000

Alarm	Attributes	Applicable major release
Name: IK4017000 (5282) Type: equipmentAlarm Package: lte.IK4017000 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INDETERMINATE OPERATIONAL FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a modem board has been detected that cannot described by any specific alarm.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1185 IK4017001

Alarm	Attributes	Applicable major release
Name: IK4017001 (5283) Type: equipmentAlarm Package: lte.IK4017001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INIT FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize a SOC of a modem board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1186 IK4017002

Alarm	Attributes	Applicable major release
Name: IK4017002 (5284) Type: equipmentAlarm Package: lte.IK4017002 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB L1 HARDWARE FAIL SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1186 IK4017002 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1187 IK4017003

Alarm	Attributes	Applicable major release
Name: IK4017003 (5285) Type: processingErrorAlarm Package: lte.IK4017003 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1188 IK4017004

Alarm	Attributes	Applicable major release
Name: IK4017004 (5286) Type: processingErrorAlarm Package: lte.IK4017004 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1189 IK4017005

Alarm	Attributes	Applicable major release
Name: IK4017005 (5287) Type: processingErrorAlarm Package: lte.IK4017005 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1190 IK4017006

Alarm	Attributes	Applicable major release
Name: IK4017006 (5288) Type: processingErrorAlarm Package: lte.IK4017006 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1191 IK4017007

Alarm	Attributes	Applicable major release
Name: IK4017007 (5289) Type: equipmentAlarm Package: lte.IK4017007 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB MODEM CELL RESOURCES FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1192 IK4017008

Alarm	Attributes	Applicable major release
Name: IK4017008 (5290) Type: processingErrorAlarm Package: lte.IK4017008 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1193 IK4017009

Alarm	Attributes	Applicable major release
Name: IK4017009 (5291) Type: processingErrorAlarm Package: lte.IK4017009 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-1193 IK4017009 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1194 IK4017010

Alarm	Attributes	Applicable major release
Name: IK4017010 (5292) Type: equipmentAlarm Package: lte.IK4017010 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 1 SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1195 IK4017011

Alarm	Attributes	Applicable major release
Name: IK4017011 (5293) Type: equipmentAlarm Package: lte.IK4017011 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 2 SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1196 IK4018000

Alarm	Attributes	Applicable major release
Name: IK4018000 (5296) Type: equipmentAlarm Package: lte.IK4018000 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INDETERMINATE OPERATIONAL FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a modem board has been detected that cannot described by any specific alarm.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1197 IK4018001

Alarm	Attributes	Applicable major release
Name: IK4018001 (5297) Type: equipmentAlarm Package: lte.IK4018001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB INIT FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize a SOC of a modem board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1198 IK4018002

Alarm	Attributes	Applicable major release
Name: IK4018002 (5298) Type: equipmentAlarm Package: lte.IK4018002 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB L1 HARDWARE FAIL SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1199 IK4018003

Alarm	Attributes	Applicable major release
Name: IK4018003 (5299) Type: processingErrorAlarm Package: lte.IK4018003 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1200 IK4018004

Alarm	Attributes	Applicable major release
Name: IK4018004 (5300) Type: processingErrorAlarm Package: lte.IK4018004 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L1 SOFTWARE FAIL SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		

Table 29-1200 IK4018004 (continued)

Alarm	Attributes	Applicable major release
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1201 IK4018005

Alarm	Attributes	Applicable major release
Name: IK4018005 (5301) Type: processingErrorAlarm Package: lte.IK4018005 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1202 IK4018006

Alarm	Attributes	Applicable major release
Name: IK4018006 (5302) Type: processingErrorAlarm Package: lte.IK4018006 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB L1 SOFTWARE WARNING SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a BB SOC unit.		
Remedial action: No action is required.		

Table 29-1203 IK4018007

Alarm	Attributes	Applicable major release
Name: IK4018007 (5303) Type: equipmentAlarm Package: lte.IK4018007 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: BB MODEM CELL RESOURCES FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1204 IK4018008

Alarm	Attributes	Applicable major release
Name: IK4018008 (5304) Type: processingErrorAlarm Package: lte.IK4018008 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1205 IK4018009

Alarm	Attributes	Applicable major release
Name: IK4018009 (5305) Type: processingErrorAlarm Package: lte.IK4018009 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: BB L2 SOFTWARE FAIL SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a BB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the BB.		

Table 29-1206 IK4018010

Alarm	Attributes	Applicable major release
Name: IK4018010 (5306) Type: equipmentAlarm Package: lte.IK4018010 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 1 SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1207 IK4018011

Alarm	Attributes	Applicable major release
Name: IK4018011 (5307) Type: equipmentAlarm Package: lte.IK4018011 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: BB FAULT 2 SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1207 IK4018011 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in.Unspecified BB fault detected on a SOC		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1208 IK4019000

Alarm	Attributes	Applicable major release
Name: IK4019000 (5310) Type: equipmentAlarm Package: lte.IK4019000 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INDETERMINATE OPERATIONAL FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a controller board has been detected that cannot described by any specific alarm.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1209 IK4019001

Alarm	Attributes	Applicable major release
Name: IK4019001 (5311) Type: equipmentAlarm Package: lte.IK4019001 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INIT FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize a SOC of a controller board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1210 IK4019002

Alarm	Attributes	Applicable major release
Name: IK4019002 (5312) Type: equipmentAlarm Package: lte.IK4019002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB L1 HARDWARE FAIL SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1211 IK4019003

Alarm	Attributes	Applicable major release
Name: IK4019003 (5313) Type: processingErrorAlarm Package: lte.IK4019003 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1212 IK4019004

Alarm	Attributes	Applicable major release
Name: IK4019004 (5314) Type: processingErrorAlarm Package: lte.IK4019004 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1213 IK4019005

Alarm	Attributes	Applicable major release
Name: IK4019005 (5315) Type: processingErrorAlarm Package: lte.IK4019005 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1214 IK4019006

Alarm	Attributes	Applicable major release
Name: IK4019006 (5316) Type: processingErrorAlarm Package: lte.IK4019006 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-1214 IK4019006 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1215 IK4019007

Alarm	Attributes	Applicable major release
Name: IK4019007 (5317) Type: equipmentAlarm Package: lte.IK4019007 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB MODEM CELL RESOURCES FAILURE SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1216 IK4019008

Alarm	Attributes	Applicable major release
Name: IK4019008 (5318) Type: processingErrorAlarm Package: lte.IK4019008 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 1-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1217 IK4019009

Alarm	Attributes	Applicable major release
Name: IK4019009 (5319) Type: processingErrorAlarm Package: lte.IK4019009 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 1-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1218 IK4019010

Alarm	Attributes	Applicable major release
Name: IK4019010 (5320) Type: equipmentAlarm Package: lte.IK4019010 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 1 SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1219 IK4019011

Alarm	Attributes	Applicable major release
Name: IK4019011 (5321) Type: equipmentAlarm Package: lte.IK4019011 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 2 SOC 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1220 IK4020000

Alarm	Attributes	Applicable major release
Name: IK4020000 (5324) Type: equipmentAlarm Package: lte.IK4020000 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INDETERMINATE OPERATIONAL FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a controller board has been detected that cannot described by any specific alarm.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1221 IK4020001

Alarm	Attributes	Applicable major release
Name: IK4020001 (5325) Type: equipmentAlarm Package: lte.IK4020001 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INIT FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1221 IK4020001 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a failure to initialize a SOC of a controller board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1222 IK4020002

Alarm	Attributes	Applicable major release
Name: IK4020002 (5326) Type: equipmentAlarm Package: lte.IK4020002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB L1 HARDWARE FAIL SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1223 IK4020003

Alarm	Attributes	Applicable major release
Name: IK4020003 (5327) Type: processingErrorAlarm Package: lte.IK4020003 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1224 IK4020004

Alarm	Attributes	Applicable major release
Name: IK4020004 (5328) Type: processingErrorAlarm Package: lte.IK4020004 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1225 IK4020005

Alarm	Attributes	Applicable major release
Name: IK4020005 (5329) Type: processingErrorAlarm Package: lte.IK4020005 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1226 IK4020006

Alarm	Attributes	Applicable major release
Name: IK4020006 (5330) Type: processingErrorAlarm Package: lte.IK4020006 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1227 IK4020007

Alarm	Attributes	Applicable major release
Name: IK4020007 (5331) Type: equipmentAlarm Package: lte.IK4020007 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB MODEM CELL RESOURCES FAILURE SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1228 IK4020008

Alarm	Attributes	Applicable major release
Name: IK4020008 (5332) Type: processingErrorAlarm Package: lte.IK4020008 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 2-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-1228 IK4020008 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1229 IK4020009

Alarm	Attributes	Applicable major release
Name: IK4020009 (5333) Type: processingErrorAlarm Package: lte.IK4020009 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 2-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1230 IK4020010

Alarm	Attributes	Applicable major release
Name: IK4020010 (5334) Type: equipmentAlarm Package: lte.IK4020010 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 1 SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1231 IK4020011

Alarm	Attributes	Applicable major release
Name: IK4020011 (5335) Type: equipmentAlarm Package: lte.IK4020011 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 2 SOC 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1232 IK4021000

Alarm	Attributes	Applicable major release
Name: IK4021000 (5338) Type: equipmentAlarm Package: lte.IK4021000 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INDETERMINATE OPERATIONAL FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a SOC modem failure of a controller board has been detected that cannot described by any specific alarm.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1233 IK4021001

Alarm	Attributes	Applicable major release
Name: IK4021001 (5339) Type: equipmentAlarm Package: lte.IK4021001 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB INIT FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize a SOC of a controller board.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1234 IK4021002

Alarm	Attributes	Applicable major release
Name: IK4021002 (5340) Type: equipmentAlarm Package: lte.IK4021002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB L1 HARDWARE FAIL SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a Layer 1 hardware or a CPRI configuration failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1235 IK4021003

Alarm	Attributes	Applicable major release
Name: IK4021003 (5341) Type: processingErrorAlarm Package: lte.IK4021003 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L

Table 29-1235 IK4021003 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1236 IK4021004

Alarm	Attributes	Applicable major release
Name: IK4021004 (5342) Type: processingErrorAlarm Package: lte.IK4021004 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L1 SOFTWARE FAIL SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1237 IK4021005

Alarm	Attributes	Applicable major release
Name: IK4021005 (5343) Type: processingErrorAlarm Package: lte.IK4021005 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1238 IK4021006

Alarm	Attributes	Applicable major release
Name: IK4021006 (5344) Type: processingErrorAlarm Package: lte.IK4021006 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB L1 SOFTWARE WARNING SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software warning on a CB SOC unit.		
Remedial action: No action is required.		

Table 29-1239 IK4021007

Alarm	Attributes	Applicable major release
Name: IK4021007 (5345) Type: equipmentAlarm Package: lte.IK4021007 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: CB MODEM CELL RESOURCES FAILURE SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a modem physical cell failure.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1240 IK4021008

Alarm	Attributes	Applicable major release
Name: IK4021008 (5346) Type: processingErrorAlarm Package: lte.IK4021008 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 3-1 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1241 IK4021009

Alarm	Attributes	Applicable major release
Name: IK4021009 (5347) Type: processingErrorAlarm Package: lte.IK4021009 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: CB L2 SOFTWARE FAIL SOC-SLICE 3-2 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates a software failure on a CB SOC unit.		
Remedial action: The faulty unit is automatically reset to attempt to clear the fault. If the problem persists then reset the eNodeB.		

Table 29-1242 IK4021010

Alarm	Attributes	Applicable major release
Name: IK4021010 (5348) Type: equipmentAlarm Package: lte.IK4021010 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 1 SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1242 IK4021010 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1243 IK4021011

Alarm	Attributes	Applicable major release
Name: IK4021011 (5349) Type: equipmentAlarm Package: lte.IK4021011 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CB FAULT 2 SOC 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected on a SOC.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1244 IK4022001

Alarm	Attributes	Applicable major release
Name: IK4022001 (7993) Type: equipmentAlarm Package: lte.IK4022001 Raised on class: lte.EthernetPort	Severity: warning Specific problem: ERRONEOUS BACKHAUL ETHERNET PORT NAME Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The backhaul port name defined in the configuration, received from the EMS by the eNB doesn't match with the identity of the ethernet backhaul port used by the eNB to connect to the EMS.		
Remedial action: EthernetPort[0].ethernetPortName value shall be modified in the EMS configuration.		

Table 29-1245 IK4022002

Alarm	Attributes	Applicable major release
Name: IK4022002 (7994) Type: qualityOfServiceAlarm Package: lte.IK4022002 Raised on class: lte.EthernetPort	Severity: major Specific problem: BAD ETHERNET PORT POLICING CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the policing ingress CIR exceeds the Ethernet port speed, when policing is requested on the Ethernet port.		

Table 29-1245 IK4022002 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Review the Ethernet port policing configuration and change if necessary.		

Table 29-1246 IK4022003

Alarm	Attributes	Applicable major release
Name: IK4022003 (7995) Type: equipmentAlarm Package: lte.IK4022003 Raised on class: lte.EthernetPort	Severity: minor Specific problem: ETHERNET PORT NOT OPERATIONAL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that a feature involving the use of this Ethernet Port has been activated and the Ethernet Port is not operational.		
Remedial action: The cabling shall be checked as well as the EMS configuration in order cabling and EMS configuration match.		

Table 29-1247 IK4022004

Alarm	Attributes	Applicable major release
Name: IK4022004 (7996) Type: equipmentAlarm Package: lte.IK4022004 Raised on class: lte.EthernetPort	Severity: indeterminate Specific problem: ETHERNET PORT OPERATIONAL Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a feature involving the use of this Ethernet Port has been activated and the Ethernet Port is operational.		
Remedial action: No action is required.		

Table 29-1248 IK4022005

Alarm	Attributes	Applicable major release
Name: IK4022005 (7997) Type: equipmentAlarm Package: lte.IK4022005 Raised on class: lte.EthernetPort	Severity: critical Specific problem: ETHERNET PORT FAILURE Implicitly cleared: true Default probable cause: inputOutputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNB failed to send/receive traffic through an Ethernet port.		
Remedial action: The eNB Ethernet port equipment shall be checked and the eNB controller board or the SFP will be replaced if necessary.		

Table 29-1249 IK4022006

Alarm	Attributes	Applicable major release
Name: IK4022006 (7998) Type: qualityOfServiceAlarm Package: lte.IK4022006 Raised on class: lte.EthernetPort	Severity: major Specific problem: BAD ETHERNET PORT SHAPING CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that either the sum of the egress CIR per VLAN exceeds the Ethernet port speed when shaping per VLAN is requested on this Ethernet port, either the egress CIR exceeds the Ethernet port speed when shaping per port is requested on this Ethernet port.		
Remedial action: Review the Ethernet port shaping configuration and change if necessary.		

Table 29-1250 IK4022007

Alarm	Attributes	Applicable major release
Name: IK4022007 (8750) Type: equipmentAlarm Package: lte.IK4022007 Raised on class: lte.EthernetPort	Severity: minor Specific problem: ETHERNET PORT FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1251 IK4022008

Alarm	Attributes	Applicable major release
Name: IK4022008 (8751) Type: equipmentAlarm Package: lte.IK4022008 Raised on class: lte.EthernetPort	Severity: minor Specific problem: ETHERNET PORT FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1252 IK4022009

Alarm	Attributes	Applicable major release
Name: IK4022009 (8752) Type: equipmentAlarm Package: lte.IK4022009 Raised on class: lte.EthernetPort	Severity: minor Specific problem: ETHERNET PORT FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1253 IK4022015

Alarm	Attributes	Applicable major release
Name: IK4022015 (10116) Type: equipmentAlarm Package: lte.IK4022015 Raised on class: lte.EthernetPort	Severity: indeterminate Specific problem: ETHERNET PORT EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-1254 IK4022016

Alarm	Attributes	Applicable major release
Name: IK4022016 (10117) Type: equipmentAlarm Package: lte.IK4022016 Raised on class: lte.EthernetPort	Severity: indeterminate Specific problem: ETHERNET PORT EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-1255 IK4022017

Alarm	Attributes	Applicable major release
Name: IK4022017 (10118) Type: equipmentAlarm Package: lte.IK4022017 Raised on class: lte.EthernetPort	Severity: indeterminate Specific problem: ETHERNET PORT EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in.		
Remedial action: No action is required.		

Table 29-1256 IK4201001

Alarm	Attributes	Applicable major release
Name: IK4201001 (2674) Type: processingErrorAlarm Package: lte.IK4201001 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: SW CANNOT BE UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download the software for the new module.		
Remedial action: Check the code server setting. The code server path is accessible via SAM or NEM. Consult the SAM resp. NEM user guide specification to see how to access the code server attribute using either application.		

Table 29-1257 IK4201002

Alarm	Attributes	Applicable major release
Name: IK4201002 (2675) Type: processingErrorAlarm Package: lte.IK4201002 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: CURRENT SW DOES NOT SUPPORT THE NEW HW MODULE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates that the current software does not support the hardware.		
Remedial action: Requires a new software package to support the hardware.		

Table 29-1258 IK4201008

Alarm	Attributes	Applicable major release
Name: IK4201008 (3229) Type: processingErrorAlarm Package: lte.IK4201008 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: SW NOT AVAILABLE, DOWNLOAD STARTED Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates that the software is not available and the download is started.		
Remedial action: Wait for download to complete.		

Table 29-1259 IK4201009

Alarm	Attributes	Applicable major release
Name: IK4201009 (3826) Type: processingErrorAlarm Package: lte.IK4201009 Raised on class: lte.CBCardSpecifics	Severity: minor Specific problem: DATA MIGRATION NOT POSSIBLE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L

Table 29-1259 IK4201009 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the not-running software does not support database migration from the actual database version. A software activation will result in fallback to minimum database.		
Remedial action: Abort the software replacement and download a compatible software package.		

Table 29-1260 IK4201010

Alarm	Attributes	Applicable major release
Name: IK4201010 (4706) Type: processingErrorAlarm Package: lte.IK4201010 Raised on class: lte.MODULE	Severity: major Specific problem: SW CANNOT BE UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download the software for the new module.		
Remedial action: Check the code server setting. The code server path is accessible via SAM or NEM. Consult the SAM resp. NEM user guide specification to see how to access the code server attribute using either application.		

Table 29-1261 IK4201011

Alarm	Attributes	Applicable major release
Name: IK4201011 (4707) Type: processingErrorAlarm Package: lte.IK4201011 Raised on class: lte.MODULE	Severity: minor Specific problem: CURRENT SW DOES NOT SUPPORT THE NEW HW MODULE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates that the current software does not support the hardware.		
Remedial action: Provide a new software package that supports the hardware.		

Table 29-1262 IK4201012

Alarm	Attributes	Applicable major release
Name: IK4201012 (4708) Type: processingErrorAlarm Package: lte.IK4201012 Raised on class: lte.MODULE	Severity: warning Specific problem: SW NOT AVAILABLE, DOWNLOAD STARTED Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates that the software is not available and the download is started.		
Remedial action: Wait for the download to complete.		

Table 29-1263 IK4201014

Alarm	Attributes	Applicable major release
Name: IK4201014 (4710) Type: processingErrorAlarm Package: lte.IK4201014 Raised on class: lte.MODULE	Severity: minor Specific problem: DATA MIGRATION NOT POSSIBLE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates that the not-running software does not support database migration from the actual database version. A software activation will result in fallback to the minimum database.		
Remedial action: Abort the software replacement and download a compatible software package.		

Table 29-1264 IK4201016

Alarm	Attributes	Applicable major release
Name: IK4201016 (8753) Type: processingErrorAlarm Package: lte.IK4201016 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1265 IK4201017

Alarm	Attributes	Applicable major release
Name: IK4201017 (8754) Type: processingErrorAlarm Package: lte.IK4201017 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1266 IK4201018

Alarm	Attributes	Applicable major release
Name: IK4201018 (8755) Type: processingErrorAlarm Package: lte.IK4201018 Raised on class: lte.RRH	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L

Table 29-1266 IK4201018 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1267 IK4201019

Alarm	Attributes	Applicable major release
Name: IK4201019 (8756) Type: processingErrorAlarm Package: lte.IK4201019 Raised on class: lte.TRDU	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1268 IK4201020

Alarm	Attributes	Applicable major release
Name: IK4201020 (8757) Type: equipmentAlarm Package: lte.IK4201020 Raised on class: lte.RetAldEntry	Severity: critical Specific problem: MISSING WORKING SOFTWARE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This alarm indicates the RET unit does not have a working application software.		
Remedial action: The unit might not recover from this alarm. A site visit might be required to replace the unit. A software download should be attempted if possible.		

Table 29-1269 IK4201021

Alarm	Attributes	Applicable major release
Name: IK4201021 (8758) Type: equipmentAlarm Package: lte.IK4201021 Raised on class: lte.TmaAldEntry	Severity: critical Specific problem: MISSING WORKING SOFTWARE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This alarm indicates the TMA unit does not have a working application software.		
Remedial action: The unit might not recover from this alarm. A site visit might be required to replace the unit. A software download should be attempted if possible.		

Table 29-1270 IK4201022

Alarm	Attributes	Applicable major release
Name: IK4201022 (8759) Type: equipmentAlarm Package: lte.IK4201022 Raised on class: lte.Rae	Severity: major Specific problem: MISSING WORKING SOFTWARE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This alarm indicates the RAE unit does not have a working application software.		
Remedial action: The unit might not recover from this alarm. A site visit might be required to replace the unit. A software download should be attempted if possible.		

Table 29-1271 IK4201023

Alarm	Attributes	Applicable major release
Name: IK4201023 (8760) Type: processingErrorAlarm Package: lte.IK4201023 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: DATA MIGRATION NOT POSSIBLE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the not-running software does not support database migration from the actual database version. A software activation will result in fallback to minimum database.		
Remedial action: Abort the software replacement and download a compatible software package.		

Table 29-1272 IK4201024

Alarm	Attributes	Applicable major release
Name: IK4201024 (8761) Type: processingErrorAlarm Package: lte.IK4201024 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: SW NOT AVAILABLE, DOWNLOAD STARTED Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the software is not available and the download is started.		
Remedial action: Wait for download to complete.		

Table 29-1273 IK4201025

Alarm	Attributes	Applicable major release
Name: IK4201025 (8762) Type: processingErrorAlarm Package: lte.IK4201025 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.RRH	Severity: minor Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1274 IK4201026

Alarm	Attributes	Applicable major release
Name: IK4201026 (8763) Type: processingErrorAlarm Package: lte.IK4201026 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: CURRENT SW DOES NOT SUPPORT THE NEW HW MODULE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the current software does not support the hardware.		
Remedial action: Requires a new software package to support the hardware.		

Table 29-1275 IK4201027

Alarm	Attributes	Applicable major release
Name: IK4201027 (8764) Type: processingErrorAlarm Package: lte.IK4201027 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: SW CANNOT BE UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to download the software for the new module.		
Remedial action: Check the code server setting. The code server path is accessible via SAM or NEM. Consult the SAM resp. NEM user guide specification to see how to access the code server attribute using either application.		

Table 29-1276 IK4201028

Alarm	Attributes	Applicable major release
Name: IK4201028 (10119) Type: processingErrorAlarm Package: lte.IK4201028 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: OAM CB FAULT 11 Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified CB fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1277 IK4201029

Alarm	Attributes	Applicable major release
Name: IK4201029 (10120) Type: processingErrorAlarm Package: lte.IK4201029 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.RRH	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure to download or activate the new software for the module.		
Remedial action: Reset the impacted module. If the alarm persists, retrigger the software download and software activation. If this is unsuccessful, contact the next level of support.		

Table 29-1278 IK4201033

Alarm	Attributes	Applicable major release
Name: IK4201033 (11026) Type: equipmentAlarm Package: lte.IK4201033 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: major Specific problem: MISSING WORKING SOFTWARE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the RET/TMA/RAE unit does not have a working application software.		
Remedial action: The unit might not recover from this alarm. A site visit might be required to replace the unit. A software download should be attempted if possible.		

Table 29-1279 IK4305001

Alarm	Attributes	Applicable major release
Name: IK4305001 (2681) Type: processingErrorAlarm Package: lte.IK4305001 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1280 IK4305002

Alarm	Attributes	Applicable major release
Name: IK4305002 (2682) Type: processingErrorAlarm Package: lte.IK4305002 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1281 IK4305003

Alarm	Attributes	Applicable major release
Name: IK4305003 (2683) Type: processingErrorAlarm Package: lte.IK4305003 Raised on class: lte.ENBShelfSpecifics	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1282 IK4305004

Alarm	Attributes	Applicable major release
Name: IK4305004 (2684) Type: processingErrorAlarm Package: lte.IK4305004 Raised on class: lte.RRH	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1283 IK4305005

Alarm	Attributes	Applicable major release
Name: IK4305005 (2685) Type: processingErrorAlarm Package: lte.IK4305005 Raised on class: lte.TRDU	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1284 IK4305006

Alarm	Attributes	Applicable major release
Name: IK4305006 (2686) Type: processingErrorAlarm Package: lte.IK4305006 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: MISSING CALLP SUBSCRIPTION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the CallP instance did not send the subscribe message due to initialization error in the CallP instance.		
Remedial action: Reset the eNodeB.		

Table 29-1285 IK4305007

Alarm	Attributes	Applicable major release
Name: IK4305007 (2687) Type: processingErrorAlarm Package: lte.IK4305007 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: MISSING CALLP REQUEST Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that there is no request from any CallP instance for the MIM status.		
Remedial action: Reset the eNodeB.		

Table 29-1286 IK4305012

Alarm	Attributes	Applicable major release
Name: IK4305012 (2692) Type: processingErrorAlarm Package: lte.IK4305012 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: INVALID CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the eNodeB configuration data.		
Remedial action: Verify and correct the configuration data.		

Table 29-1287 IK4305013

Alarm	Attributes	Applicable major release
Name: IK4305013 (2693) Type: processingErrorAlarm Package: lte.IK4305013 Raised on class: lte.MmeTransportLayerAccess	Severity: major Specific problem: IP ADDRESS CONFIGURATION DATA MISMATCH Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the IP address is not well filled for the ipFormat specified in Vlan		
Remedial action: Verify and correct the configuration data.		

Table 29-1288 IK4305014

Alarm	Attributes	Applicable major release
Name: IK4305014 (2694) Type: processingErrorAlarm Package: lte.IK4305014 Raised on class: lte.X2TransportLayerAccess	Severity: major Specific problem: IP ADDRESS CONFIGURATION DATA MISMATCH Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the IP address is not well filled for the ipFormat specified in Vlan		
Remedial action: Verify and correct the configuration data.		

Table 29-1289 IK4305016

Alarm	Attributes	Applicable major release
Name: IK4305016 (2696) Type: processingErrorAlarm Package: lte.IK4305016 Raised on class: lte.RRH	Severity: minor Specific problem: PRIMARY CPRI PORT CONFIGURATION MISMATCH Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the misalignment between primary CPRI port position in MIM configuration and real CPRI port position detected		
Remedial action: Verify and correct the configuration data or Verify and correct the hardware configuration		

Table 29-1290 IK4305017

Alarm	Attributes	Applicable major release
Name: IK4305017 (2697) Type: processingErrorAlarm Package: lte.IK4305017 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: INVALID TRANSPORT CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an inconsistency in the eNodeB transport configuration data.		
Remedial action: Verify and correct the configuration data if needed		

Table 29-1291 IK4305018

Alarm	Attributes	Applicable major release
Name: IK4305018 (2698) Type: processingErrorAlarm Package: lte.IK4305018 Raised on class: lte.ENBEquipment	Severity: major Specific problem: PRIMARY IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the primary IPsec tunnel.		
Remedial action: Check the IP Security configuration.		

Table 29-1292 IK4305019

Alarm	Attributes	Applicable major release
Name: IK4305019 (2699) Type: processingErrorAlarm Package: lte.IK4305019 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: SECONDARY IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the secondary IPsec tunnel.		
Remedial action: Check the IP Security configuration.		

Table 29-1293 IK4305020

Alarm	Attributes	Applicable major release
Name: IK4305020 (2700) Type: equipmentAlarm Package: lte.IK4305020 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FACTORY MODE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1293 IK4305020 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the eNodeB is not completely configured.		
Remedial action: Complete the eNodeB configuration.		

Table 29-1294 IK4305021

Alarm	Attributes	Applicable major release
Name: IK4305021 (2701) Type: equipmentAlarm Package: lte.IK4305021 Raised on class: lte.RRH	Severity: minor Specific problem: VSWR CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the thresholds of the VSWR configuration could not be applied to the eNodeB.		
Remedial action: Verify the correctness of the configuration data. Apply again the data. Reset the eNodeB if it fails.		

Table 29-1295 IK4305022

Alarm	Attributes	Applicable major release
Name: IK4305022 (2702) Type: equipmentAlarm Package: lte.IK4305022 Raised on class: lte.TRDU	Severity: minor Specific problem: VSWR CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the thresholds of the VSWR configuration could not be applied to the eNodeB.		
Remedial action: Verify the correctness of the configuration data. Apply again the data. Reset the eNodeB if it fails.		

Table 29-1296 IK4305023

Alarm	Attributes	Applicable major release
Name: IK4305023 (2703) Type: processingErrorAlarm Package: lte.IK4305023 Raised on class: lte.Cell	Severity: critical Specific problem: DELAY TIMING OUT OF RANGE Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the delay timing values is out of range.		
Remedial action: 1 - Lock the cell. 2 - Verify the correctness of the configuration data. 3 - Unlock the cell.		

Table 29-1297 IK4305024

Alarm	Attributes	Applicable major release
Name: IK4305024 (2704) Type: processingErrorAlarm Package: lte.IK4305024 Raised on class: lte.AMR	Severity: minor Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1298 IK4305025

Alarm	Attributes	Applicable major release
Name: IK4305025 (2705) Type: processingErrorAlarm Package: lte.IK4305025 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1299 IK4305026

Alarm	Attributes	Applicable major release
Name: IK4305026 (2706) Type: processingErrorAlarm Package: lte.IK4305026 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1300 IK4305027

Alarm	Attributes	Applicable major release
Name: IK4305027 (2707) Type: processingErrorAlarm Package: lte.IK4305027 Raised on class: lte.ENBEquipment	Severity: major Specific problem: IP ADDRESS CONFIGURATION DATA MISMATCH Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB performed an autonomous fallback to the previous transport configuration due to lack of OAM connectivity.		

Table 29-1300 IK4305027 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify and correct the configuration data.		

Table 29-1301 IK4305028

Alarm	Attributes	Applicable major release
Name: IK4305028 (2708) Type: processingErrorAlarm Package: lte.IK4305028 Raised on class: lte.Cell	Severity: critical Specific problem: TOTAL ROUND TRIP DELAY EXCEEDED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB measured total round trip delay exceeds the predefined maximum allowed value as determined by licensing.		
Remedial action: Verify setting of isFiberDelayAllowed is consistent with length of BBU to radio link. Parameter isFiberDelayAllowed must be True if BBU to radio link exceeds 500 meters. Verify antennaPathDelayDL and antennaPathDelayUL parameter values. Parameter isDasDelayEnabled must be True if antenna delay exceeds 2100 nanoseconds.		

Table 29-1302 IK4305029

Alarm	Attributes	Applicable major release
Name: IK4305029 (2709) Type: processingErrorAlarm Package: lte.IK4305029 Raised on class: lte.Cell	Severity: warning Specific problem: DELAY COMPENSATION WARNING Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB delay compensation is not accurate enough.		
Remedial action: Verify delay compensation parameters.		

Table 29-1303 IK4305030

Alarm	Attributes	Applicable major release
Name: IK4305030 (2710) Type: processingErrorAlarm Package: lte.IK4305030 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY CHECK RADIOCAC FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1303 IK4305030 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the configuration parameters, number of users per cell and/or number of data bearers per cell, exceed the HW or SW capabilities of the modem.		
Remedial action: Verify and correct the configuration data.		

Table 29-1304 IK4305031

Alarm	Attributes	Applicable major release
Name: IK4305031 (2711) Type: processingErrorAlarm Package: lte.IK4305031 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY CHECK CELL FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configured bandwidth and/or downlink power of the cell and /or band ID is not in line with the HW capabilities.		
Remedial action: Verify and correct the configuration data.		

Table 29-1305 IK4305032

Alarm	Attributes	Applicable major release
Name: IK4305032 (2712) Type: processingErrorAlarm Package: lte.IK4305032 Raised on class: lte.Cell	Severity: warning Specific problem: HW SW CAPABILITY CHECK DOWNGRADE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configuration data is inconsistent with the HW and SW capabilities of the eNodeB. OAM has downgraded the configured data to be in line with the HW and SW capabilities.		
Remedial action: Verify and correct the configuration data.		

Table 29-1306 IK4305033

Alarm	Attributes	Applicable major release
Name: IK4305033 (2713) Type: processingErrorAlarm Package: lte.IK4305033 Raised on class: lte.Cell	Severity: critical Specific problem: DELAY COMPENSATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB is unable to compute a valid downlink/uplink frame offset value for the modem.		

Table 29-1306 IK4305033 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the fiber length between the controller board and the remote radio head. Verify the antenna cable length. Verify the delay compensation parameters.		

Table 29-1307 IK4305034

Alarm	Attributes	Applicable major release
Name: IK4305034 (2714) Type: processingErrorAlarm Package: lte.IK4305034 Raised on class: lte.Cell	Severity: critical Specific problem: DELAY COMPENSATION HW CAPABILITY FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB is unable to compute a valid downlink/uplink frame offset value for the modem because of hardware constraints.		
Remedial action: Verify the hardware capabilities of the controller and of the remote radio head.		

Table 29-1308 IK4305035

Alarm	Attributes	Applicable major release
Name: IK4305035 (3230) Type: equipmentAlarm Package: lte.IK4305035 Raised on class: lte.Cell	Severity: warning Specific problem: MISSING MODEM RESOURCES FOR CONFIGURED LTECELL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there are not enough modem resources available to support the configured cell.		
Remedial action: Verify and correct the configuration data.		

Table 29-1309 IK4305036

Alarm	Attributes	Applicable major release
Name: IK4305036 (3231) Type: equipmentAlarm Package: lte.IK4305036 Raised on class: lte.Cell	Severity: warning Specific problem: MISSING RFM FOR CONFIGURED LTECELL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that there are no sectors or RFMs available to support the configured cell.		
Remedial action: Verify and correct the configuration data.		

Table 29-1310 IK4305037

Alarm	Attributes	Applicable major release
Name: IK4305037 (3232) Type: equipmentAlarm Package: lte.IK4305037 Raised on class: lte.RRH	Severity: warning Specific problem: RFM EQUIPPED WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that there is a RRH equipped but no cell is mapped on the sector.		
Remedial action: Verify and correct the configuration data.		

Table 29-1311 IK4305038

Alarm	Attributes	Applicable major release
Name: IK4305038 (3233) Type: equipmentAlarm Package: lte.IK4305038 Raised on class: lte.TRDU	Severity: warning Specific problem: RFM EQUIPPED WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that there is a TRDU equipped but no cell is mapped on the sector.		
Remedial action: Verify and correct the configuration data.		

Table 29-1312 IK4305039

Alarm	Attributes	Applicable major release
Name: IK4305039 (3234) Type: equipmentAlarm Package: lte.IK4305039 Raised on class: lte.BBCardSpecifics	Severity: warning Specific problem: BB EQUIPPED WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there is a modem equipped but no cell is mapped.		
Remedial action: Verify and correct the configuration data.		

Table 29-1313 IK4305040

Alarm	Attributes	Applicable major release
Name: IK4305040 (3235) Type: equipmentAlarm Package: lte.IK4305040 Raised on class: lte.Cell	Severity: warning Specific problem: HW SW CAPABILITY ANTENNA CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the antenna configuration data is inconsistent with the hardware and software capabilities of the eNodeB.		
Remedial action: Verify and correct the configuration data.		

Table 29-1314 IK4305041

Alarm	Attributes	Applicable major release
Name: IK4305041 (3236) Type: equipmentAlarm Package: lte.IK4305041 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY DLEARFCN VIOLATE LOWER BANDEDGE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configured downlink EARFCN with the configured bandwidth violate the lower operating band edge.		
Remedial action: Verify and correct the configuration data.		

Table 29-1315 IK4305042

Alarm	Attributes	Applicable major release
Name: IK4305042 (3237) Type: equipmentAlarm Package: lte.IK4305042 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY DLEARFCN VIOLATE UPPER BANDEDGE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configured downlink EARFCN with the configured bandwidth violate the upper operating band edge.		
Remedial action: Verify and correct the configuration data.		

Table 29-1316 IK4305043

Alarm	Attributes	Applicable major release
Name: IK4305043 (3238) Type: equipmentAlarm Package: lte.IK4305043 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY ULEARFCN VIOLATE LOWER BANDEDGE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configured uplink EARFCN with the configured bandwidth violate the lower operating band edge.		
Remedial action: Verify and correct the configuration data.		

Table 29-1317 IK4305044

Alarm	Attributes	Applicable major release
Name: IK4305044 (3239) Type: equipmentAlarm Package: lte.IK4305044 Raised on class: lte.Cell	Severity: major Specific problem: HW SW CAPABILITY ULEARFCN VIOLATE UPPER BANDEDGE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configured uplink EARFCN with the configured bandwidth violate the upper operating band edge.		
Remedial action: Verify and correct the configuration data.		

Table 29-1318 IK4305045

Alarm	Attributes	Applicable major release
Name: IK4305045 (3240) Type: equipmentAlarm Package: lte.IK4305045 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: HW SW CAPABILITY RACK DOES NOT SUPPORT MODEM Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the equipped modem version is not support by dbu rack version.		
Remedial action: Verify and correct the equipment configuration.		

Table 29-1319 IK4305047

Alarm	Attributes	Applicable major release
Name: IK4305047 (3242) Type: equipmentAlarm Package: lte.IK4305047 Raised on class: lte.ENBEquipment	Severity: major Specific problem: CDMA PHASE SYNC HOLDOVER TIMER EXPIRED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the phase sync holdover time expired. The LTE to HRPD enhanced non optimized handover is no longer possible.		
Remedial action: Resolve faulty references.		

Table 29-1320 IK4305048

Alarm	Attributes	Applicable major release
Name: IK4305048 (3243) Type: processingErrorAlarm Package: lte.IK4305048 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: CT NOT STARTED DUE TO ACTIVE DDT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that call trace could not be started because dynamic debug trace is already active.		
Remedial action: Verify and correct the configuration data.		

Table 29-1321 IK4305049

Alarm	Attributes	Applicable major release
Name: IK4305049 (3244) Type: processingErrorAlarm Package: lte.IK4305049 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: DDT NOT STARTED DUE TO ACTIVE CT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that dynamic debug trace could not be started because call trace is already active.		
Remedial action: Verify and correct the configuration data.		

Table 29-1322 IK4305050

Alarm	Attributes	Applicable major release
Name: IK4305050 (3245) Type: processingErrorAlarm Package: lte.IK4305050 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: TRACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the trace server destination could not be configured.		
Remedial action: Verify and correct the configuration data. If the problem persists, reset the eNodeB.		

Table 29-1323 IK4305051

Alarm	Attributes	Applicable major release
Name: IK4305051 (3246) Type: processingErrorAlarm Package: lte.IK4305051 Raised on class: lte.Cell	Severity: critical Specific problem: UNCOMPLETE ENB SCENARIO RELATED TO CELL Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the Cell Setup scenario failed due to a missing or incomplete internal action.		
Remedial action: Perform lock/unlock on the impacted cell. If needed, perform eNodeB reset.		

Table 29-1324 IK4305052

Alarm	Attributes	Applicable major release
Name: IK4305052 (3247) Type: equipmentAlarm Package: lte.IK4305052 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE UNLIMITED PRB LICENSE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, feature UnlimitedPRBLicense is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1325 IK4305053

Alarm	Attributes	Applicable major release
Name: IK4305053 (3248) Type: equipmentAlarm Package: lte.IK4305053 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE MOBILITY TO 1XRTT NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, MobilityTo1xRTT feature disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1326 IK4305054

Alarm	Attributes	Applicable major release
Name: IK4305054 (3249) Type: equipmentAlarm Package: lte.IK4305054 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE UE CATEGORY 4 NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, UeCategory4 feature disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1327 IK4305055

Alarm	Attributes	Applicable major release
Name: IK4305055 (3250) Type: equipmentAlarm Package: lte.IK4305055 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE SPS NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, Sps feature is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1328 IK4305056

Alarm	Attributes	Applicable major release
Name: IK4305056 (3251) Type: equipmentAlarm Package: lte.IK4305056 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE ROHC NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, Rohc feature is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1329 IK4305059

Alarm	Attributes	Applicable major release
Name: IK4305059 (3254) Type: equipmentAlarm Package: lte.IK4305059 Raised on class: lte.Cell	Severity: warning Specific problem: FEATURE 4 RX DIVERSITY NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature 4RxDiversity mismatch, LteCell is operating in degraded mode.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1330 IK4305060

Alarm	Attributes	Applicable major release
Name: IK4305060 (3255) Type: equipmentAlarm Package: lte.IK4305060 Raised on class: lte.Cell	Severity: warning Specific problem: FEATURE SYNC SIGNALS DIVERSITY NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, SyncSignalsDiversity feature is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1331 IK4305061

Alarm	Attributes	Applicable major release
Name: IK4305061 (3256) Type: equipmentAlarm Package: lte.IK4305061 Raised on class: lte.Cell	Severity: warning Specific problem: FEATURE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, feature is disabled by OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1332 IK4305065

Alarm	Attributes	Applicable major release
Name: IK4305065 (3260) Type: processingErrorAlarm Package: lte.IK4305065 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA SOFTWARE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the software download to the TMA unit failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1333 IK4305066

Alarm	Attributes	Applicable major release
Name: IK4305066 (3261) Type: processingErrorAlarm Package: lte.IK4305066 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET SOFTWARE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the software download to the RET unit failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1334 IK4305067

Alarm	Attributes	Applicable major release
Name: IK4305067 (3262) Type: processingErrorAlarm Package: lte.IK4305067 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET ANTENNA CONFIGURATION FILE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1334 IK4305067 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the configuration file download to the RET unit failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1335 IK4305068

Alarm	Attributes	Applicable major release
Name: IK4305068 (3263) Type: equipmentAlarm Package: lte.IK4305068 Raised on class: lte.Cell	Severity: warning Specific problem: ANTENNA PATH LOST Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that at least one antenna path of that cell is lost and that the cell operates in degraded mode (e.g. SIMO/SISO instead of MIMO).		
Remedial action: Verify the antennas and the RFM, belonging to the cell.		

Table 29-1336 IK4305069

Alarm	Attributes	Applicable major release
Name: IK4305069 (3264) Type: processingErrorAlarm Package: lte.IK4305069 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: UNKNOWN FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the OAM layer of the eNodeB received an unknown fault from another software layer. A specific handling of this unknown fault is not possible. Eventually available information about the unknown fault is provided in the alarm additional information attribute.		
Remedial action: Contact the next level of support.		

Table 29-1337 IK4305070

Alarm	Attributes	Applicable major release
Name: IK4305070 (3265) Type: processingErrorAlarm Package: lte.IK4305070 Raised on class: lte.Cell	Severity: warning Specific problem: 3GPP TEST MODE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that during the configuration of the 3GPP test mode the call processing layer or the modem software failed to process the provided configuration.		

Table 29-1337 IK4305070 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check and correct the configuration data. Lock/unlock the cell. If the problem persists, contact the next level support.		

Table 29-1338 IK4305071

Alarm	Attributes	Applicable major release
Name: IK4305071 (3266) Type: equipmentAlarm Package: lte.IK4305071 Raised on class: lte.Cell	Severity: warning Specific problem: CELL DIV IMBALANCE THRESHOLD EXCEEDED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a diversity imbalance threshold crossing across the two or more RX paths of the cell. One or more receive paths or antennas are no longer operating at normal performance.		
Remedial action: Perform a study of root causes. Contact the Field support if necessary.		

Table 29-1339 IK4305073

Alarm	Attributes	Applicable major release
Name: IK4305073 (3268) Type: processingErrorAlarm Package: lte.IK4305073 Raised on class: lte.Cell	Severity: warning Specific problem: OAM CELL FAULT 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1340 IK4305076

Alarm	Attributes	Applicable major release
Name: IK4305076 (3271) Type: processingErrorAlarm Package: lte.IK4305076 Raised on class: lte.Cell	Severity: warning Specific problem: OAM CELL FAULT 5 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1341 IK4305077

Alarm	Attributes	Applicable major release
Name: IK4305077 (3664) Type: equipmentAlarm Package: lte.IK4305077 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE GEO LOC PHASE SYNCH NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, Geo loc phase synch feature is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1342 IK4305078

Alarm	Attributes	Applicable major release
Name: IK4305078 (3665) Type: equipmentAlarm Package: lte.IK4305078 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE IMS EMERGENCY CALL NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature mismatch, IMS emergency call feature is disabled by eNodeB OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1343 IK4305079

Alarm	Attributes	Applicable major release
Name: IK4305079 (3666) Type: equipmentAlarm Package: lte.IK4305079 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE RACH 2 FORMAT NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature RACH 2 format mismatch, LteCell is disabled by OAM.		
Remedial action: 1 - Lock the cell. 2 - Ensure compatibility between the eNodeB configuration data and the equipped modem type. 3 - Unlock the cell.		

Table 29-1344 IK4305080

Alarm	Attributes	Applicable major release
Name: IK4305080 (3667) Type: equipmentAlarm Package: lte.IK4305080 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE DAS DELAY NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature DAS delay mismatch, LteCell is disabled by OAM.		
Remedial action: 1 - Lock the cell. 2 -Ensure compatibility between the eNodeB configuration data and the equipped modem type. 3 - Unlock the cell.		

Table 29-1345 IK4305082

Alarm	Attributes	Applicable major release
Name: IK4305082 (3669) Type: equipmentAlarm Package: lte.IK4305082 Raised on class: lte.Cell	Severity: major Specific problem: ALL ANTENNA PATHS LOST Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that all antenna paths of that cell are lost and that the cell is disabled.		
Remedial action: Verify the antennas and the RFM, belonging to the cell.		

Table 29-1346 IK4305083

Alarm	Attributes	Applicable major release
Name: IK4305083 (3670) Type: equipmentAlarm Package: lte.IK4305083 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE LONG FIBER NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a modem type feature long fiber delay mismatch, LteCell is disabled by OAM.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1347 IK4305084

Alarm	Attributes	Applicable major release
Name: IK4305084 (3671) Type: equipmentAlarm Package: lte.IK4305084 Raised on class: lte.RFM	Severity: major Specific problem: INCOMPATIBLE CONFIGURATION MAJOR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The LTE controller has encountered an error while configuring this RE, possibly due to an incompatibility in the interface between controller and RE. As a result a cell assigned to this RE cannot be configured and activated.		
Remedial action: Reconfigure the RE to correct the value of any parameter described in the alarm additional information.		

Table 29-1348 IK4305085

Alarm	Attributes	Applicable major release
Name: IK4305085 (3672) Type: equipmentAlarm Package: lte.IK4305085 Raised on class: lte.RFM	Severity: warning Specific problem: INCOMPATIBLE CONFIGURATION WARNING Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The LTE controller has encountered an error while configuring the RE but the cell(s) on this RE can still be activated.		
Remedial action: Reconfigure the RE to correct the value of any parameter described in the alarm additional information. If this is a multistandard RE and the parameter applies to a common resource of the RE then the value must be Unset.		

Table 29-1349 IK4305086

Alarm	Attributes	Applicable major release
Name: IK4305086 (3673) Type: equipmentAlarm Package: lte.IK4305086 Raised on class: lte.RFM	Severity: minor Specific problem: LOCAL CELL POWER LIMIT EXCEEDED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: The downlink total power for a cell assigned to this RE exceeds the Local Cell Power Limit set at installation time.		
Remedial action: Reconfigure the cell of this RE: set the power to be less than or equal to the local cell power limit defined for this MSRE at installation time.		

Table 29-1350 IK4305088

Alarm	Attributes	Applicable major release
Name: IK4305088 (3828) Type: processingErrorAlarm Package: lte.IK4305088 Raised on class: lte.RRH	Severity: warning Specific problem: CONFIGURATION DATA MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the eNodeB configuration data versus the equipped hardware.		
Remedial action: Verify and correct the configuration data. Verify and correct the hardware configuration		

Table 29-1351 IK4305089

Alarm	Attributes	Applicable major release
Name: IK4305089 (3829) Type: processingErrorAlarm Package: lte.IK4305089 Raised on class: lte.TRDU	Severity: warning Specific problem: CONFIGURATION DATA MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the eNodeB configuration data versus the equipped hardware.		
Remedial action: Verify and correct the configuration data. Verify and correct the hardware configuration		

Table 29-1352 IK4305090

Alarm	Attributes	Applicable major release
Name: IK4305090 (3830) Type: processingErrorAlarm Package: lte.IK4305090 Raised on class: lte.AntennaPort	Severity: warning Specific problem: CONFIGURATION DATA MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the eNodeB configuration data versus the equipped hardware.		
Remedial action: Verify and correct the configuration data. Verify and correct the hardware configuration		

Table 29-1353 IK4305091

Alarm	Attributes	Applicable major release
Name: IK4305091 (3831) Type: processingErrorAlarm Package: lte.IK4305091 Raised on class: lte.AntennaPort	Severity: warning Specific problem: HW SW CAPABILITY CHECK ANTENNA PORT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the eNodeB AntennaPort configuration data		
Remedial action: Verify and correct the configuration data.		

Table 29-1354 IK4305092

Alarm	Attributes	Applicable major release
Name: IK4305092 (3832) Type: processingErrorAlarm Package: lte.IK4305092 Raised on class: lte.ENBEquipment	Severity: major Specific problem: CMS INIT FAILED (ERROR) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates CMS(Certificate Management Support) initialization request failure due to an error.		
Remedial action: Check the Sub CMS configuration. Verify and correct the CMS configuration data based on the error code received. Check the network connection. eNB has to get the valid operator-signed certificate(s) before the concerned traffic can be resumed.		

Table 29-1355 IK4305093

Alarm	Attributes	Applicable major release
Name: IK4305093 (3833) Type: processingErrorAlarm Package: lte.IK4305093 Raised on class: lte.ENBEquipment	Severity: major Specific problem: CMS INIT FAILED (TIMEOUT) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates CMS(Certificate Management Support) initialization request failure due to timeout.		
Remedial action: eNB has to get the valid operator-signed certificate(s) before the concerned traffic can be resumed.\nCheck the network connection, then check IP connectivity, HTTP connectivity and Sub CMS/CMS server connectivity.\nCheck the Sub CMS/CMS configuration.		

Table 29-1356 IK4305094

Alarm	Attributes	Applicable major release
Name: IK4305094 (3834) Type: processingErrorAlarm Package: lte.IK4305094 Raised on class: lte.ENBEquipment	Severity: major Specific problem: CMS KEY UPDATE FAILED (ERROR) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates CMS(Certificate Management Support) key update failure due to an error.		
Remedial action: Check the Sub CMS configuration. Verify and correct the CMS configuration data based on the error code received.		

Table 29-1357 IK4305095

Alarm	Attributes	Applicable major release
Name: IK4305095 (3835) Type: processingErrorAlarm Package: lte.IK4305095 Raised on class: lte.ENBEquipment	Severity: major Specific problem: CMS KEY UPDATE FAILED (TIMEOUT) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates CMS(Certificate Management Support) key update activity failure due to timeout.		
Remedial action: The eNodeB did not receive a message response back from the Sub-CMS during a CMP message exchange.\nThe timeout could be because the Sub CMS is not online or the CMS IP address was incorrect or the network is down or some other failure reason.		

Table 29-1358 IK4305097

Alarm	Attributes	Applicable major release
Name: IK4305097 (3837) Type: processingErrorAlarm Package: lte.IK4305097 Raised on class: lte.ENBEquipment	Severity: major Specific problem: OPERATOR CERTIFICATE ENROLLMENT ERROR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that certificate enrollment can not be started because no authentication credentials were found.		
Remedial action: Provide the shared key for authentication of CMPv2 messages . eNodeB uses a shared key for authentication to Sub CMS when performing certificate enrollment.		

Table 29-1359 IK4305099

Alarm	Attributes	Applicable major release
Name: IK4305099 (3839) Type: equipmentAlarm Package: lte.IK4305099 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE eMBMS NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration for eMBMS feature is not supported by equipped modem type		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1360 IK4305100

Alarm	Attributes	Applicable major release
Name: IK4305100 (3840) Type: equipmentAlarm Package: lte.IK4305100 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: FEATURE TTI BUNDLING FOR VoIP NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration for TTI bundling for VoIP feature is not supported by equipped modem type		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1361 IK4305101

Alarm	Attributes	Applicable major release
Name: IK4305101 (3841) Type: equipmentAlarm Package: lte.IK4305101 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE DUAL-BAND NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration with dual band ID is not supported by equipped modem type		
Remedial action: Verify and correct the configuration data.		

Table 29-1362 IK4305102

Alarm	Attributes	Applicable major release
Name: IK4305102 (3842) Type: equipmentAlarm Package: lte.IK4305102 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE DUPLEX MODE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration duplex-mode is not supported by equipped modem type		
Remedial action: To clear the alarm, revert to previous mode		

Table 29-1363 IK4305103

Alarm	Attributes	Applicable major release
Name: IK4305103 (3843) Type: equipmentAlarm Package: lte.IK4305103 Raised on class: lte.Cell	Severity: warning Specific problem: FEATURE OP-PUCCH NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration for OP-PUCCH is not supported by equipped modem type		
Remedial action: Verify and correct the configuration data.		

Table 29-1364 IK4305104

Alarm	Attributes	Applicable major release
Name: IK4305104 (3844) Type: equipmentAlarm Package: lte.IK4305104 Raised on class: lte.Cell	Severity: critical Specific problem: HW SW CAPABILITY DOWNLINK CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell DL configuration is not supported by equipped modem type		
Remedial action: Verify and correct the configuration data.		

Table 29-1365 IK4305105

Alarm	Attributes	Applicable major release
Name: IK4305105 (3845) Type: equipmentAlarm Package: lte.IK4305105 Raised on class: lte.BBCardSpecifics	Severity: critical Specific problem: FEATURE 3 MHZ NOT SUPPORTED BY MODEM TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that modem type does not support 3 MHz bandwidth.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1366 IK4305106

Alarm	Attributes	Applicable major release
Name: IK4305106 (3846) Type: processingErrorAlarm Package: lte.IK4305106 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #4 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#4).		
Remedial action: Check the IP Security configuration.		

Table 29-1367 IK4305107

Alarm	Attributes	Applicable major release
Name: IK4305107 (3847) Type: processingErrorAlarm Package: lte.IK4305107 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #5 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#5).		
Remedial action: Check the IP Security configuration.		

Table 29-1368 IK4305108

Alarm	Attributes	Applicable major release
Name: IK4305108 (3848) Type: processingErrorAlarm Package: lte.IK4305108 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #6 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1368 IK4305108 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure of the IPsec tunnel (#6).		
Remedial action: Check the IP Security configuration.		

Table 29-1369 IK4305109

Alarm	Attributes	Applicable major release
Name: IK4305109 (3849) Type: processingErrorAlarm Package: lte.IK4305109 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #7 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#7).		
Remedial action: Check the IP Security configuration.		

Table 29-1370 IK4305110

Alarm	Attributes	Applicable major release
Name: IK4305110 (3850) Type: processingErrorAlarm Package: lte.IK4305110 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #8 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#8).		
Remedial action: Check the IP Security configuration.		

Table 29-1371 IK4305111

Alarm	Attributes	Applicable major release
Name: IK4305111 (3851) Type: processingErrorAlarm Package: lte.IK4305111 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #9 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#9).		
Remedial action: Check the IP Security configuration.		

Table 29-1372 IK4305112

Alarm	Attributes	Applicable major release
Name: IK4305112 (3852) Type: processingErrorAlarm Package: lte.IK4305112 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #10 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#10).		
Remedial action: Check the IP Security configuration.		

Table 29-1373 IK4305116

Alarm	Attributes	Applicable major release
Name: IK4305116 (5352) Type: processingErrorAlarm Package: lte.IK4305116 Raised on class: lte.RRH	Severity: minor Specific problem: SECONDARY CPRI PORT CONFIGURATION MISMATCH Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the misalignment between secondary CPRI port position in MIM configuration and real secondary CPRI port position detected.		
Remedial action: Verify and correct the configuration data or Verify and correct the hardware configuration		

Table 29-1374 IK4305117

Alarm	Attributes	Applicable major release
Name: IK4305117 (5353) Type: processingErrorAlarm Package: lte.IK4305117 Raised on class: lte.Cell	Severity: major Specific problem: CELL ANTENNA PORT NUMBER MISMATCH VERSUS MODEM LOAD TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the DL/UL antenna number configured for this Cell mismatch with Modem load. Triggers for raising the alarm:\n1. If (LteCell->numberofULAntennas ="=8 Or CellActivationService.IsMultiRRHEnabled=True) AND EnbTDD. Is8AloadNeeded=False\n2. If (LteCell->numberofULAntennas!=8 AND CellActivationService.IsMultiRRHEnabled=False) AND EnbTDD.Is8AloadNeeded=True\nTriggers for clear the alarm:\n1. If (LteCell->numberofULAntennas ==8 Or CellActivationService. IsMultiRRHEnabled=True) AND EnbTDD.Is8AloadNeeded=True \n2. If (LteCell->numberofULAntennas!=8 AND CellActivationService. IsMultiRRHEnabled=False) AND EnbTDD.Is8AloadNeeded= False"		
Remedial action: Online modify parameter is8ALoadNeeded on EnbTDD object or modify DL/UL antenna number configuration of LteCell to make them consistent.		

Table 29-1375 IK4305118

Alarm	Attributes	Applicable major release
Name: IK4305118 (5354) Type: communicationsAlarm Package: lte.IK4305118 Raised on class: lte.M3MmeTransportLayerAccess	Severity: indeterminate Specific problem: M3 LINK RESET DUE ON-LINE M3-INTERFACE CLASS PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates M3 link has reset when operator updates the value of M3-interface Class parameter on-line.		
Remedial action: No action is required.		

Table 29-1376 IK4305119

Alarm	Attributes	Applicable major release
Name: IK4305119 (4714) Type: processingErrorAlarm Package: lte.IK4305119 Raised on class: lte.Cell	Severity: major Specific problem: AUTOMATED HANDOVER PARAMETER ADIUSTMENT NOT POSSIBLE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the SON process that automatically adjusts intra-frequency handover parameters cannot make any adjustments because of the setting of the configurable limits on the allowed adjustments.		
Remedial action: Modify the handover parameter adjustment limits to allow additional values.		

Table 29-1377 IK4305120

Alarm	Attributes	Applicable major release
Name: IK4305120 (4715) Type: equipmentAlarm Package: lte.IK4305120 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: TOTAL LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates that the eICIC functionality is being disabled due to very large clock drift		
Remedial action: Check the timing source of the eNB		

Table 29-1378 IK4305121

Alarm	Attributes	Applicable major release
Name: IK4305121 (4716) Type: equipmentAlarm Package: lte.IK4305121 Raised on class: lte.MODULE	Severity: major Specific problem: TOTAL LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L
Description: This alarm indicates that the eICIC functionality is being disabled due to very large clock drift		
Remedial action: Check the timing source of the eNB		

Table 29-1379 IK4305126

Alarm	Attributes	Applicable major release
Name: IK4305126 (4720) Type: processingErrorAlarm Package: lte.IK4305126 Raised on class: lte.Cell	Severity: major Specific problem: CELL MAJOR CONFIGURATION ERROR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates there is a major error in the configuration of the cell.		
Remedial action: Operator must set the attribute(s) in error to a value consistent with the configuration of the LteCell.		

Table 29-1380 IK4305127

Alarm	Attributes	Applicable major release
Name: IK4305127 (4721) Type: processingErrorAlarm Package: lte.IK4305127 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ENB WARNING CONFIGURATION ERROR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates there is a warning error in the configuration of the eNB.		
Remedial action: Operator should set the attribute(s) in error to a value consistent with the configuration of the eNB.		

Table 29-1381 IK4305128

Alarm	Attributes	Applicable major release
Name: IK4305128 (5355) Type: processingErrorAlarm Package: lte.IK4305128 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: RFTRACE NOT STARTED DUE TO ACTIVE DDT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RF trace could not be started because dynamic debug trace is already active.		
Remedial action: Verify and correct the configuration data.		

Table 29-1382 IK4305130

Alarm	Attributes	Applicable major release
Name: IK4305130 (4723) Type: processingErrorAlarm Package: lte.IK4305130 Raised on class: lte.MODULE	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1383 IK4305131

Alarm	Attributes	Applicable major release
Name: IK4305131 (4724) Type: processingErrorAlarm Package: lte.IK4305131 Raised on class: lte.MODULE	Severity: critical Specific problem: MISSING CALLP SUBSCRIPTION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the CallP instance did not send the subscribe message due to initialization error in the CallP instance.		
Remedial action: Reset the eNodeB.		

Table 29-1384 IK4305132

Alarm	Attributes	Applicable major release
Name: IK4305132 (4725) Type: processingErrorAlarm Package: lte.IK4305132 Raised on class: lte.MODULE	Severity: critical Specific problem: MISSING CALLP REQUEST Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1384 IK4305132 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that there is no request from any CallP instance for the MIM status.		
Remedial action: Reset the eNodeB.		

Table 29-1385 IK4305134

Alarm	Attributes	Applicable major release
Name: IK4305134 (4727) Type: processingErrorAlarm Package: lte.IK4305134 Raised on class: lte.MODULE	Severity: critical Specific problem: INVALID CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the eNodeB configuration data.		
Remedial action: Verify and correct the configuration data.		

Table 29-1386 IK4305135

Alarm	Attributes	Applicable major release
Name: IK4305135 (4728) Type: processingErrorAlarm Package: lte.IK4305135 Raised on class: lte.MODULE	Severity: critical Specific problem: INVALID TRANSPORT CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an inconsistency in the eNodeB transport configuration data.		
Remedial action: Verify and correct the configuration data.		

Table 29-1387 IK4305136

Alarm	Attributes	Applicable major release
Name: IK4305136 (4729) Type: processingErrorAlarm Package: lte.IK4305136 Raised on class: lte.MODULE	Severity: warning Specific problem: UNKNOWN FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the OAM layer of the eNodeB received an unknown fault from another software layer.		
Remedial action: Refer to the alarm additional information for further detail, contact the next level of support.		

Table 29-1388 IK4305137

Alarm	Attributes	Applicable major release
Name: IK4305137 (4730) Type: processingErrorAlarm Package: lte.IK4305137 Raised on class: lte.MODULE	Severity: major Specific problem: RESET DATABASE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to restore database.		
Remedial action: Contact the next level of support.		

Table 29-1389 IK4305138

Alarm	Attributes	Applicable major release
Name: IK4305138 (4731) Type: equipmentAlarm Package: lte.IK4305138 Raised on class: lte.MODULE	Severity: major Specific problem: CELL CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to configure the cell.		
Remedial action: Verify the cell configuration data. Reset the modem and allocate the cell resources.		

Table 29-1390 IK4305139

Alarm	Attributes	Applicable major release
Name: IK4305139 (4732) Type: equipmentAlarm Package: lte.IK4305139 Raised on class: lte.MODULE	Severity: warning Specific problem: MODEM FUNCTION AVAILABLE WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there is a modem function equipped but no cell is mapped to the modem.		
Remedial action: Verify and correct the configuration data.		

Table 29-1391 IK4305140

Alarm	Attributes	Applicable major release
Name: IK4305140 (4733) Type: equipmentAlarm Package: lte.IK4305140 Raised on class: lte.MODULE	Severity: critical Specific problem: EXPECTED MODEM NOT EQUIPPED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that equipped modem type does not fit the expectedModemType in the database.		
Remedial action: Modify the database to correctly describe the modem hardware.		

Table 29-1392 IK4305142

Alarm	Attributes	Applicable major release
Name: IK4305142 (4734) Type: equipmentAlarm Package: lte.IK4305142 Raised on class: lte.MODULE	Severity: critical Specific problem: OAM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the OAM interface.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-1393 IK4305143

Alarm	Attributes	Applicable major release
Name: IK4305143 (4735) Type: equipmentAlarm Package: lte.IK4305143 Raised on class: lte.MODULE	Severity: critical Specific problem: TELECOM INTERFACE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the IP and Ethernet configuration on the telecom interface.		
Remedial action: Reset the eNodeB. If the alarm persists, contact the next level of support.		

Table 29-1394 IK4305144

Alarm	Attributes	Applicable major release
Name: IK4305144 (4736) Type: equipmentAlarm Package: lte.IK4305144 Raised on class: lte.MODULE	Severity: critical Specific problem: SSH SERVER START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1394 IK4305144 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the failure to start the SSH server.		
Remedial action: Reset the eNodeB.		

Table 29-1395 IK4305145

Alarm	Attributes	Applicable major release
Name: IK4305145 (4737) Type: equipmentAlarm Package: lte.IK4305145 Raised on class: lte.MODULE	Severity: minor Specific problem: SNTP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to start the SNTP client.		
Remedial action: Check the network connectivity of NTP server and NTP server address provisioning. If the NTP server is unreachable or the provisioning is incorrect, address those aspects. If all other possible causes have been eliminated, reset the eNodeB.		

Table 29-1396 IK4305146

Alarm	Attributes	Applicable major release
Name: IK4305146 (4738) Type: equipmentAlarm Package: lte.IK4305146 Raised on class: lte.MODULE	Severity: critical Specific problem: DHCP CLIENT START FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to start the DHCP client on the eNodeB network interface.		
Remedial action: Reset the eNodeB.		

Table 29-1397 IK4305147

Alarm	Attributes	Applicable major release
Name: IK4305147 (4739) Type: processingErrorAlarm Package: lte.IK4305147 Raised on class: lte.MODULE	Severity: minor Specific problem: UNEXPECTED DATA FROM DHCP SERVER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the lease time offered by the DHCP server is different from the lease time requested by the DHCP client.		
Remedial action: Configure the DHCP server with an infinite lease time.		

Table 29-1398 IK4305149

Alarm	Attributes	Applicable major release
Name: IK4305149 (4741) Type: equipmentAlarm Package: lte.IK4305149 Raised on class: lte.MODULE	Severity: critical Specific problem: SCTP INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to initialize the SCTP access.		
Remedial action: Reset the eNodeB.		

Table 29-1399 IK4305151

Alarm	Attributes	Applicable major release
Name: IK4305151 (4743) Type: equipmentAlarm Package: lte.IK4305151 Raised on class: lte.MODULE	Severity: critical Specific problem: END OF THE HOLDOVER DURATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: The internal oscillator is not being disciplined by the reference source and its frequency drift may soon exceed allowed limits. This holdover duration is dependent on the type of oscillator.		
Remedial action: Fix the timing reference source.		

Table 29-1400 IK4305153

Alarm	Attributes	Applicable major release
Name: IK4305153 (5356) Type: processingErrorAlarm Package: lte.IK4305153 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #3 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a failure of IPsec tunnel (#3).		
Remedial action: Check the IP Security configuration.		

Table 29-1401 IK4305154

Alarm	Attributes	Applicable major release
Name: IK4305154 (5357) Type: equipmentAlarm Package: lte.IK4305154 Raised on class: lte.Cell	Severity: critical Specific problem: CELL CONFIGURATION DATA MISMATCH VERSUS CORRESPONDING FEATURE DEACTIVATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the cell configuration data mismatch versus corresponding feature deactivation.		
Remedial action: Verify and correct the configuration data.		

Table 29-1402 IK4305155

Alarm	Attributes	Applicable major release
Name: IK4305155 (4745) Type: equipmentAlarm Package: lte.IK4305155 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM SCB FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1403 IK4305156

Alarm	Attributes	Applicable major release
Name: IK4305156 (4746) Type: equipmentAlarm Package: lte.IK4305156 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM SCB FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1404 IK4305157

Alarm	Attributes	Applicable major release
Name: IK4305157 (4747) Type: equipmentAlarm Package: lte.IK4305157 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM SCB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1404 IK4305157 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1405 IK4305158

Alarm	Attributes	Applicable major release
Name: IK4305158 (4748) Type: equipmentAlarm Package: lte.IK4305158 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM MODEM FUNCTION FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1406 IK4305160

Alarm	Attributes	Applicable major release
Name: IK4305160 (4750) Type: equipmentAlarm Package: lte.IK4305160 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM MODEM FUNCTION FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1407 IK4305161

Alarm	Attributes	Applicable major release
Name: IK4305161 (4751) Type: equipmentAlarm Package: lte.IK4305161 Raised on class: lte.MODULE	Severity: critical Specific problem: FEATURE 3 MHZ NOT SUPPORTED BY MODEM TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that modem type does not support 3 MHz bandwidth.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1408 IK4305162

Alarm	Attributes	Applicable major release
Name: IK4305162 (4752) Type: communicationsAlarm Package: lte.IK4305162 Raised on class: lte.MODULE	Severity: major Specific problem: ETHERNET TRANSPORT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an interface error due to the counters exceeding the configured threshold.		
Remedial action: Check the network status and cabling if possible. If the alarm persists, contact the next level support.		

Table 29-1409 IK4305163

Alarm	Attributes	Applicable major release
Name: IK4305163 (4753) Type: equipmentAlarm Package: lte.IK4305163 Raised on class: lte.MODULE	Severity: major Specific problem: DHCP CLIENT LEASE FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure of the DHCP client to obtain the lease from the DHCP server.		
Remedial action: Check for connectivity. Check for DHCP server and network configurations.		

Table 29-1410 IK4305164

Alarm	Attributes	Applicable major release
Name: IK4305164 (4754) Type: equipmentAlarm Package: lte.IK4305164 Raised on class: lte.MODULE	Severity: warning Specific problem: IP LOOPBACK ACTIVE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the IP loopback is activated.		
Remedial action: Call the next level of support.		

Table 29-1411 IK4305165

Alarm	Attributes	Applicable major release
Name: IK4305165 (4755) Type: processingErrorAlarm Package: lte.IK4305165 Raised on class: lte.RFME	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an internal procedure failure due to no response from the module.		
Remedial action: Reset the eNB. If the alarm persists, replace the module.		

Table 29-1412 IK4305166

Alarm	Attributes	Applicable major release
Name: IK4305166 (4756) Type: equipmentAlarm Package: lte.IK4305166 Raised on class: lte.RFME	Severity: minor Specific problem: OAM RFME FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1413 IK4305167

Alarm	Attributes	Applicable major release
Name: IK4305167 (4757) Type: equipmentAlarm Package: lte.IK4305167 Raised on class: lte.RFME	Severity: minor Specific problem: OAM RFME FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1414 IK4305168

Alarm	Attributes	Applicable major release
Name: IK4305168 (4758) Type: equipmentAlarm Package: lte.IK4305168 Raised on class: lte.RFME	Severity: minor Specific problem: OAM RFME FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1415 IK4305169

Alarm	Attributes	Applicable major release
Name: IK4305169 (4759) Type: equipmentAlarm Package: lte.IK4305169 Raised on class: lte.RFME	Severity: minor Specific problem: VSWR CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the thresholds of the VSWR configuration could not be applied to the eNodeB.		

Table 29-1415 IK4305169 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the correctness of the configuration data and apply the data again. If this fails to correct the fault then reset the eNodeB.		

Table 29-1416 IK4305170

Alarm	Attributes	Applicable major release
Name: IK4305170 (4760) Type: equipmentAlarm Package: lte.IK4305170 Raised on class: lte.RFME	Severity: warning Specific problem: RFME AVAILABLE WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there is RFME equipped but no cell is mapped.		
Remedial action: Verify and correct the configuration data.		

Table 29-1417 IK4305171

Alarm	Attributes	Applicable major release
Name: IK4305171 (4761) Type: equipmentAlarm Package: lte.IK4305171 Raised on class: lte.RFME	Severity: minor Specific problem: LOCAL CELL POWER LIMIT EXCEEDED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: The downlink total power for a cell assigned to this RE exceeds the Local Cell Power Limit set at installation time.		
Remedial action: Reconfigure the cell of this RE: set the power to be less than or equal to the local cell power limit defined for this MSRE at installation time.		

Table 29-1418 IK4305172

Alarm	Attributes	Applicable major release
Name: IK4305172 (4762) Type: equipmentAlarm Package: lte.IK4305172 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1419 IK4305173

Alarm	Attributes	Applicable major release
Name: IK4305173 (4763) Type: equipmentAlarm Package: lte.IK4305173 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1420 IK4305174

Alarm	Attributes	Applicable major release
Name: IK4305174 (4764) Type: equipmentAlarm Package: lte.IK4305174 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1421 IK4305177

Alarm	Attributes	Applicable major release
Name: IK4305177 (4765) Type: processingErrorAlarm Package: lte.IK4305177 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: RESET DATABASE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to restore database.		
Remedial action: Contact the next level of support.		

Table 29-1422 IK4305178

Alarm	Attributes	Applicable major release
Name: IK4305178 (4766) Type: processingErrorAlarm Package: lte.IK4305178 Raised on class: lte.RFME	Severity: warning Specific problem: CONFIGURATION DATA MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L

Table 29-1422 IK4305178 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates inconsistency in the eNodeB configuration data versus the equipped hardware.		
Remedial action: Verify and correct the configuration data. Verify and correct the hardware configuration		

Table 29-1423 IK4305179

Alarm	Attributes	Applicable major release
Name: IK4305179 (4767) Type: processingErrorAlarm Package: lte.IK4305179 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: CERTIFICATE EXPIRED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The eNodeB discovered an expired certificate during validity date audit. Re-install or reconfigure the eNodeB so that key pair creation and certificate enrollment with the CMS are performed again.		
Remedial action: Trigger the certificate enrollment to generate new certificates.		

Table 29-1424 IK4305180

Alarm	Attributes	Applicable major release
Name: IK4305180 (4768) Type: equipmentAlarm Package: lte.IK4305180 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE CARRIER AGGREGATION NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration with Carrier Aggregation is not supported by the equipped modem type.		
Remedial action: Verify and correct the configuration data.		

Table 29-1425 IK4305181

Alarm	Attributes	Applicable major release
Name: IK4305181 (4769) Type: equipmentAlarm Package: lte.IK4305181 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE SIX CELLS NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration with six cells with single carrier is not supported by the equipped modem type.		

Table 29-1425 IK4305181 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify and correct the configuration data.		

Table 29-1426 IK4305184

Alarm	Attributes	Applicable major release
Name: IK4305184 (5358) Type: processingErrorAlarm Package: lte.IK4305184 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: RFTRACE STOPPED DUE TO ACTIVE DDT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that RF trace has stopped because dynamic debug trace has been activated.		
Remedial action: Verify and correct the configuration data.		

Table 29-1427 IK4305185

Alarm	Attributes	Applicable major release
Name: IK4305185 (5359) Type: processingErrorAlarm Package: lte.IK4305185 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CMS INIT START Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that operator certificate enrollment scenario started.		
Remedial action: No action is required.		

Table 29-1428 IK4305186

Alarm	Attributes	Applicable major release
Name: IK4305186 (5360) Type: equipmentAlarm Package: lte.IK4305186 Raised on class: lte.Cell	Severity: critical Specific problem: CPRI LICENSE REQUIRED TO SUPPORT BANDWIDTH FOR CONFIGURED LTECELL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the required CPRI line rate to support the bandwidth of the configured cell can not be achieved due to licensing restriction.		
Remedial action: The operator shall purchase the license for CPRI rate 5		

Table 29-1429 IK4305187

Alarm	Attributes	Applicable major release
Name: IK4305187 (7999) Type: processingErrorAlarm Package: lte.IK4305187 Raised on class: lte.RRH	Severity: minor Specific problem: TERTIARY CPRI PORT CONFIGURATION MISMATCH Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the misalignment between the tertiary CPRI port position in MIM configuration and the detected tertiary CPRI port position, or the tertiary CPRI port is configured but the RRH cannot support 3 ports at all.		
Remedial action: Verify and correct the configuration data or Verify and correct the hardware configuration, or verify if RRH support 3 CPRI ports.		

Table 29-1430 IK4305188

Alarm	Attributes	Applicable major release
Name: IK4305188 (8000) Type: processingErrorAlarm Package: lte.IK4305188 Raised on class: lte.Cell	Severity: critical Specific problem: CELL OR SECTOR CONFIGURATION MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the cell or corresponding sector configuration versus the RRH hardware capacity		
Remedial action: Verify and correct the configuration data or Verify and correct the hardware configuration		

Table 29-1431 IK4305189

Alarm	Attributes	Applicable major release
Name: IK4305189 (8001) Type: processingErrorAlarm Package: lte.IK4305189 Raised on class: lte.Cell	Severity: major Specific problem: LTE NEIGHBOR RELATION MIB INSTANCE CANNOT BE REMOVED BY ANR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the LTE neighbor relation MIB instance is not removed because the removal is not allowed.		
Remedial action: Remove the existing LTE neighbor relation so that it can be created by ANR under the correct frequency.		

Table 29-1432 IK4305190

Alarm	Attributes	Applicable major release
Name: IK4305190 (8002) Type: equipmentAlarm Package: lte.IK4305190 Raised on class: lte.Cell	Severity: critical Specific problem: LICENSE REQUIRED TO SUPPORT THE CONFIGURED LTECELL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell cannot be enabled due to licensing restriction		
Remedial action: The operator shall purchase the corresponding license.		

Table 29-1433 IK4305191

Alarm	Attributes	Applicable major release
Name: IK4305191 (8003) Type: processingErrorAlarm Package: lte.IK4305191 Raised on class: lte.Cell	Severity: critical Specific problem: 4TX CELL CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a cell is configured with 4 DL antennas, whereas the feature allowing 4 Tx antennas is disabled (is4TxAntennasEnabled="false)."		
Remedial action: Verify the DL antennas setting for this cell in MIM and verify the is4TxAntennasEnabled flag in MIM.		

Table 29-1434 IK4305192

Alarm	Attributes	Applicable major release
Name: IK4305192 (8004) Type: processingErrorAlarm Package: lte.IK4305192 Raised on class: lte.RFM	Severity: major Specific problem: CONFIGURATION DATA REJECTED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates inconsistency in the RFM configuration data.		
Remedial action: Verify and correct the configuration data. Identify from additional info the impacted parameter.		

Table 29-1435 IK4305193

Alarm	Attributes	Applicable major release
Name: IK4305193 (8765) Type: processingErrorAlarm Package: lte.IK4305193 Raised on class: lte.Cell	Severity: indeterminate Specific problem: OAM CELL EVENT 8 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This event is for future use.		
Remedial action: No action is required.		

Table 29-1436 IK4305194

Alarm	Attributes	Applicable major release
Name: IK4305194 (8766) Type: equipmentAlarm Package: lte.IK4305194 Raised on class: lte.Rae	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1437 IK4305195

Alarm	Attributes	Applicable major release
Name: IK4305195 (8767) Type: processingErrorAlarm Package: lte.IK4305195 Raised on class: lte.Rae	Severity: major Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1438 IK4305201

Alarm	Attributes	Applicable major release
Name: IK4305201 (8768) Type: processingErrorAlarm Package: lte.IK4305201 Raised on class: lte.Cell	Severity: critical Specific problem: CELL NOT OPERATIONAL DUE TO RF PATH FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the cell is not operational due to RF path critical failure.		

Table 29-1438 IK4305201 (continued)

Alarm	Attributes	Applicable major release
Remedial action: If the alarm persists, the cell is disabled.		

Table 29-1439 IK4305206

Alarm	Attributes	Applicable major release
Name: IK4305206 (8769) Type: equipmentAlarm Package: lte.IK4305206 Raised on class: lte.Cell	Severity: critical Specific problem: CANNOT ASSIGN LTECELL TO TARGET MODEM TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell cannot be enabled because it cannot be assigned to the specified target modem type.		
Remedial action: Either change the parameter targetModemType or reconnect the CPRI link of the Radio Equipment managing this cell. The rule being the following:\nWhen targetModemType =" bCEM, then the Radio Equipment managing this cell shall be connected to eCCM(2) board\nWhen targetModemType = bCxM2, then the Radio Equipment managing this cell shall be connected to a bCAM2 or bCEM2\nWhen targetModemType is unset, then the expectedModemType shall be different from bCEM, bCxM2 and bCEMorBCxM2"		

Table 29-1440 IK4305207

Alarm	Attributes	Applicable major release
Name: IK4305207 (8770) Type: equipmentAlarm Package: lte.IK4305207 Raised on classes: • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: LRA WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a local recovery action of the modem physical cell resource.		
Remedial action: No action is required.		

Table 29-1441 IK4305208

Alarm	Attributes	Applicable major release
Name: IK4305208 (8771) Type: equipmentAlarm Package: lte.IK4305208 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1441 IK4305208 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the main RF antenna position coordinates might not be correct.		
Remedial action: No action is required.		

Table 29-1442 IK4305209

Alarm	Attributes	Applicable major release
Name: IK4305209 (8772) Type: equipmentAlarm Package: lte.IK4305209 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the main RF antenna position coordinates have changed. The GPS antenna of the eNodeB has been moved or the mainAntennaPositionDeltaX/Y/Z values have been reconfigured.		
Remedial action: No action is required.		

Table 29-1443 IK4305210

Alarm	Attributes	Applicable major release
Name: IK4305210 (8773) Type: equipmentAlarm Package: lte.IK4305210 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BBU POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the BBU position coordinates have changed. The GPS antenna of the eNodeB has been moved or the bbuPositionDeltaX/Y/Z coordinates have been reconfigured.		
Remedial action: No action is required.		

Table 29-1444 IK4305211

Alarm	Attributes	Applicable major release
Name: IK4305211 (8774) Type: equipmentAlarm Package: lte.IK4305211 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BBU POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the BBU position coordinates might not be correct.		
Remedial action: No action is required.		

Table 29-1445 IK4305212

Alarm	Attributes	Applicable major release
Name: IK4305212 (8775) Type: equipmentAlarm Package: lte.IK4305212 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates an OAM auto-reset with an empty database as the database was not restored properly.		
Remedial action: No action is required.		

Table 29-1446 IK4305213

Alarm	Attributes	Applicable major release
Name: IK4305213 (8776) Type: equipmentAlarm Package: lte.IK4305213 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the controller board is reset to restore the configuration data.		
Remedial action: No action is required.		

Table 29-1447 IK4305214

Alarm	Attributes	Applicable major release
Name: IK4305214 (8777) Type: equipmentAlarm Package: lte.IK4305214 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER OAM ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1448 IK4305215

Alarm	Attributes	Applicable major release
Name: IK4305215 (8778) Type: equipmentAlarm Package: lte.IK4305215 Raised on classes: • lte.ENBEquipment • lte.MODULE	Severity: indeterminate Specific problem: RESET ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1449 IK4305216

Alarm	Attributes	Applicable major release
Name: IK4305216 (8779) Type: communicationsAlarm Package: lte.IK4305216 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: DATABASE RECONFIGURATION RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a reset was performed due to a database reconfiguration.		
Remedial action: No action is required.		

Table 29-1450 IK4305217

Alarm	Attributes	Applicable major release
Name: IK4305217 (8780) Type: equipmentAlarm Package: lte.IK4305217 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.ENBEquipment • lte.Rae • lte.TmaAldEntry • lte.RRH	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1451 IK4305218

Alarm	Attributes	Applicable major release
Name: IK4305218 (8781) Type: equipmentAlarm Package: lte.IK4305218 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RFME • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.TmaAldEntry • lte.RRH	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1452 IK4305219

Alarm	Attributes	Applicable major release
Name: IK4305219 (8782) Type: processingErrorAlarm Package: lte.IK4305219 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: RESET DATABASE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to restore database.		
Remedial action: Contact the next level of support.		

Table 29-1453 IK4305220

Alarm	Attributes	Applicable major release
Name: IK4305220 (8783) Type: equipmentAlarm Package: lte.IK4305220 Raised on classes: • lte.BBCardSpecifics • lte.MODULE	Severity: critical Specific problem: FEATURE 3 MHZ NOT SUPPORTED BY MODEM TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that modem type does not support 3 MHz bandwidth.		
Remedial action: Ensure compatibility between the eNodeB configuration data and the equipped modem type.		

Table 29-1454 IK4305222

Alarm	Attributes	Applicable major release
Name: IK4305222 (8784) Type: processingErrorAlarm Package: lte.IK4305222 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: warning Specific problem: UNKNOWN FAULT Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the OAM layer of the eNodeB received an unknown fault from another software layer. A specific handling of this unknown fault is not possible. Eventually available information about the unknown fault is provided in the alarm additional information attribute.		
Remedial action: Contact the next level of support.		

Table 29-1455 IK4305223

Alarm	Attributes	Applicable major release
Name: IK4305223 (8785) Type: equipmentAlarm Package: lte.IK4305223 Raised on classes: • lte.TRDU • lte.RRH	Severity: warning Specific problem: RFM EQUIPPED WITHOUT LTECELL CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that there is a RRH equipped but no cell is mapped on the sector.		
Remedial action: Verify and correct the configuration data.		

Table 29-1456 IK4305224

Alarm	Attributes	Applicable major release
Name: IK4305224 (8786) Type: equipmentAlarm Package: lte.IK4305224 Raised on classes: • lte.RFME • lte.TRDU • lte.RRH	Severity: minor Specific problem: VSWR CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the thresholds of the VSWR configuration could not be applied to the eNodeB.		
Remedial action: Verify the correctness of the configuration data. Apply again the data. Reset the eNodeB if it fails.		

Table 29-1457 IK4305225

Alarm	Attributes	Applicable major release
Name: IK4305225 (8787) Type: processingErrorAlarm Package: lte.IK4305225 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: INVALID TRANSPORT CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates an inconsistency in the eNodeB transport configuration data.		
Remedial action: Verify and correct the configuration data.		

Table 29-1458 IK4305226

Alarm	Attributes	Applicable major release
Name: IK4305226 (8788) Type: processingErrorAlarm Package: lte.IK4305226 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: INVALID CONFIGURATION DATA Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the eNodeB configuration data.		
Remedial action: Verify and correct the configuration data.		

Table 29-1459 IK4305229

Alarm	Attributes	Applicable major release
Name: IK4305229 (8789) Type: processingErrorAlarm Package: lte.IK4305229 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: MISSING CALLP REQUEST Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there is no request from any CallP instance for the MIM status.		
Remedial action: Reset the eNodeB.		

Table 29-1460 IK4305230

Alarm	Attributes	Applicable major release
Name: IK4305230 (8790) Type: processingErrorAlarm Package: lte.IK4305230 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: MISSING CALLP SUBSCRIPTION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the CallP instance did not send the subscribe message due to initialization error in the CallP instance.		
Remedial action: Reset the eNodeB.		

Table 29-1461 IK4305231

Alarm	Attributes	Applicable major release
Name: IK4305231 (8791) Type: processingErrorAlarm Package: lte.IK4305231 Raised on classes: • lte.ENBShelfSpecifics • lte.CBCardSpecifics • lte.RFME • lte.RetAldEntry • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.TmaAldEntry • lte.AMR • lte.Rae • lte.RRH	Severity: critical Specific problem: MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1462 IK4305232

Alarm	Attributes	Applicable major release
Name: IK4305232 (8792) Type: processingErrorAlarm Package: lte.IK4305232 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODEM RESET DUE ON-LINE B-MODEM CLASS PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates Modem has reset when operator updates the value of B-Modem Class parameter on-line.		
Remedial action: No action is required.		

Table 29-1463 IK4305233

Alarm	Attributes	Applicable major release
Name: IK4305233 (8793) Type: equipmentAlarm Package: lte.IK4305233 Raised on class: lte.Cell	Severity: warning Specific problem: CELL CONFIGURATION DATA MISMATCH VERSUS RFM HW CAPABILITIES Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1463 IK4305233 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the cell configuration data mismatch versus corresponding RFM Hw Capabilities.		
Remedial action: Verify and correct the configuration data.		

Table 29-1464 IK4305234

Alarm	Attributes	Applicable major release
Name: IK4305234 (10122) Type: processingErrorAlarm Package: lte.IK4305234 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: CT/MDT NOT STARTED DUE TO ACTIVE DDT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that call trace or MDT could not be started because dynamic debug trace is already active.		
Remedial action: Verify and correct the configuration data.		

Table 29-1465 IK4305235

Alarm	Attributes	Applicable major release
Name: IK4305235 (10123) Type: processingErrorAlarm Package: lte.IK4305235 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: CT/MDT STOPPED DUE TO ACTIVE DDT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that call trace or MDT is stopped because dynamic debug trace is activated.		
Remedial action: Verify and correct the configuration data.		

Table 29-1466 IK4305236

Alarm	Attributes	Applicable major release
Name: IK4305236 (10124) Type: communicationsAlarm Package: lte.IK4305236 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 6 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-1467 IK4305237

Alarm	Attributes	Applicable major release
Name: IK4305237 (10125) Type: communicationsAlarm Package: lte.IK4305237 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM CB EVENT 7 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: No action is required.		

Table 29-1468 IK4305244

Alarm	Attributes	Applicable major release
Name: IK4305244 (10126) Type: processingErrorAlarm Package: lte.IK4305244 Raised on class: lte.Cell	Severity: minor Specific problem: OAM CELL FAULT 6 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1469 IK4305245

Alarm	Attributes	Applicable major release
Name: IK4305245 (10127) Type: processingErrorAlarm Package: lte.IK4305245 Raised on class: lte.Cell	Severity: major Specific problem: OAM CELL FAULT 7 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1470 IK4305246

Alarm	Attributes	Applicable major release
Name: IK4305246 (10128) Type: communicationsAlarm Package: lte.IK4305246 Raised on class: lte.M3MmeTransportLayerAccess	Severity: indeterminate Specific problem: M3 TRANS EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS event detected.		

Table 29-1470 IK4305246 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1471 IK4305247

Alarm	Attributes	Applicable major release
Name: IK4305247 (10129) Type: communicationsAlarm Package: lte.IK4305247 Raised on class: lte.M3MmeTransportLayerAccess	Severity: indeterminate Specific problem: M3 TRANS EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS event detected.		
Remedial action: No action is required.		

Table 29-1472 IK4305248

Alarm	Attributes	Applicable major release
Name: IK4305248 (10130) Type: communicationsAlarm Package: lte.IK4305248 Raised on class: lte.M3MmeTransportLayerAccess	Severity: indeterminate Specific problem: M3 TRANS EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS event detected.		
Remedial action: No action is required.		

Table 29-1473 IK4305252

Alarm	Attributes	Applicable major release
Name: IK4305252 (10131) Type: operationalViolation Package: lte.IK4305252 Raised on class: lte.Cell	Severity: critical Specific problem: INCORRECT BW-REDUCTION CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: When the isCompactBandwidthEnable="TRUE and pass activation checks, ENB will configure RRH with 4 different BWReduction parameters. In case configuring at least 1 of these parameters failed, OAM will stop the Cell setup scenario and raise this fault."		
Remedial action: There are 2 options: \n- Configure BWReduction parameters to supported value by RRH \n- or, disable the feature (isCompactBandwidthEnable="FALSE)"		

Table 29-1474 IK4305253

Alarm	Attributes	Applicable major release
Name: IK4305253 (10132) Type: equipmentAlarm Package: lte.IK4305253 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SRIO SWITCH BOX RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates the reset command by the operator.		
Remedial action: None.		

Table 29-1475 IK4305254

Alarm	Attributes	Applicable major release
Name: IK4305254 (10133) Type: processingErrorAlarm Package: lte.IK4305254 Raised on classes: • lte.RFM • lte.CBCardSpecifics • lte.AMR	Severity: major Specific problem: CONFIGURATION DATA REJECTED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the module configuration data.		
Remedial action: Verify and correct the configuration data. Identify from additional info the impacted parameter.		

Table 29-1476 IK4305257

Alarm	Attributes	Applicable major release
Name: IK4305257 (11027) Type: operationalViolation Package: lte.IK4305257 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE CAT-M NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates there is a critical error in the configuration of the cell. The cell configuration with CAT-M is not supported.		
Remedial action: Operator must set the attribute(s) in error to a value consistent with the configuration of the LteCell.		

Table 29-1477 IK4305258

Alarm	Attributes	Applicable major release
Name: IK4305258 (11028) Type: equipmentAlarm Package: lte.IK4305258 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: LRA WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates a local recovery action of the modem physical cell resource.		
Remedial action: No action is required.		

Table 29-1478 IK4305259

Alarm	Attributes	Applicable major release
Name: IK4305259 (11029) Type: equipmentAlarm Package: lte.IK4305259 Raised on class: lte.TmaAldEntry	Severity: major Specific problem: TMA MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1479 IK4305260

Alarm	Attributes	Applicable major release
Name: IK4305260 (11030) Type: equipmentAlarm Package: lte.IK4305260 Raised on class: lte.AMR	Severity: minor Specific problem: AMR MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1480 IK4305261

Alarm	Attributes	Applicable major release
Name: IK4305261 (11031) Type: equipmentAlarm Package: lte.IK4305261 Raised on class: lte.ENBShelfSpecifics	Severity: minor Specific problem: DBU MODULE SCENARIO ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1480 IK4305261 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates the scenario failure due to no-response from the module.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1481 IK4306000

Alarm	Attributes	Applicable major release
Name: IK4306000 (5361) Type: equipmentAlarm Package: lte.IK4306000 Raised on class: lte.RFM	Severity: indeterminate Specific problem: UNEXPECTED RF MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned failure on the RFM. \n More detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for the support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact the support for further assistance.		
Remedial action: No action is required.		

Table 29-1482 IK4306002

Alarm	Attributes	Applicable major release
Name: IK4306002 (4773) Type: processingErrorAlarm Package: lte.IK4306002 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SESSION STOP FAILURE AT ENB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the Session Stop procedure has failed at eNB level.		
Remedial action: No action is required.		

Table 29-1483 IK4306003

Alarm	Attributes	Applicable major release
Name: IK4306003 (4774) Type: operationalViolation Package: lte.IK4306003 Raised on class: lte.Cell	Severity: indeterminate Specific problem: MBSFN - POSITIONNING REFERENCE SIGNAL COLLISION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1483 IK4306003 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the set of sub-frames allocated by the MCE for eMBMS services overwrites some sub-frames dedicated to Positioning reference signals.		
Remedial action: No action is required.		

Table 29-1484 IK4306004

Alarm	Attributes	Applicable major release
Name: IK4306004 (4775) Type: operationalViolation Package: lte.IK4306004 Raised on class: lte.Cell	Severity: indeterminate Specific problem: MBSFN - ABS SUB-FRAME COLLISON Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the set of sub-frames allocated by the MCE for eMBMS services includes some Almost Blank Subframes reserved for the eICIC feature.		
Remedial action: No action is required.		

Table 29-1485 IK4306005

Alarm	Attributes	Applicable major release
Name: IK4306005 (4776) Type: qualityOfServiceAlarm Package: lte.IK4306005 Raised on class: lte.Cell	Severity: major Specific problem: LACK OF UNICAST RESOURCES DUE TO EMBMS RESOURCE ALLOCATION Implicitly cleared: true Default probable cause: congestion	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the amount of sub-frames needed by the unicast bearers is exceeding the configured threshold.		
Remedial action: Multiple actions are possible: (1) use a greater value of unicastPercentUsageThreshold (2) use a larger value of unicastCongestionTime (3) reserve more resources for eMBMS in eNB admission control (percentMcastReservedPRB) (4) limit the eMBMS resources over the different MBSFN areas in the MCE configuration (5) set up external equipments so that they can notify the MCE of session start with more anticipation and unicast bearers have more time to disconnect		

Table 29-1486 IK4306006

Alarm	Attributes	Applicable major release
Name: IK4306006 (4777) Type: equipmentAlarm Package: lte.IK4306006 Raised on class: lte.ENBEquipment	Severity: major Specific problem: NETCONF QUEUE LIMIT EXCEEDED Implicitly cleared: true Default probable cause: queueSizeExceeded	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1486 IK4306006 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that one or more DB update request messages received from eNB CallP has been discarded by eNB OAM due to Netconf queue exceeding its limit. The alarm is cleared when no messages have been discarded for 5 minutes.		
Remedial action: Remove any PCI related mismatches using WPS checks (specifically check Nei_Lte_0003)		

Table 29-1487 IK4306008

Alarm	Attributes	Applicable major release
Name: IK4306008 (4779) Type: processingErrorAlarm Package: lte.IK4306008 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #11 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#11).		
Remedial action: Check the IP Security configuration.		

Table 29-1488 IK4306009

Alarm	Attributes	Applicable major release
Name: IK4306009 (4780) Type: processingErrorAlarm Package: lte.IK4306009 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #12 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#12).		
Remedial action: Check the IP Security configuration.		

Table 29-1489 IK4306010

Alarm	Attributes	Applicable major release
Name: IK4306010 (4781) Type: processingErrorAlarm Package: lte.IK4306010 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #13 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#13).		
Remedial action: Check the IP Security configuration.		

Table 29-1490 IK4306011

Alarm	Attributes	Applicable major release
Name: IK4306011 (4782) Type: processingErrorAlarm Package: lte.IK4306011 Raised on class: lte.ENBEquipment	Severity: major Specific problem: #14 IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel (#14).		
Remedial action: Check the IP Security configuration.		

Table 29-1491 IK4306014

Alarm	Attributes	Applicable major release
Name: IK4306014 (4999) Type: equipmentAlarm Package: lte.IK4306014 Raised on class: lte.Cell	Severity: critical Specific problem: INSUFFICIENT CPRI IQ RESOURCE FOR CONFIGURED LTECELL Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there are no cpri IQ resource available to support the configured cell.		
Remedial action: Check any HW(SFP, RRH type, CB type) impact on CPRI IQ resource. If HW is correct, verify and correct the configuration data.		

Table 29-1492 IK4306015

Alarm	Attributes	Applicable major release
Name: IK4306015 (5362) Type: processingErrorAlarm Package: lte.IK4306015 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: INVALID TIME ZONE NAME Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB could not be configured with the requested time zone.		
Remedial action: Operator may select another equivalent time zone value, e.g. try Etc/GMT+x or Etc/GMT-x instead of the requested Area/Location, or contact their next level of technical support.		

Table 29-1493 IK4306016

Alarm	Attributes	Applicable major release
Name: IK4306016 (5363) Type: processingErrorAlarm Package: lte.IK4306016 Raised on class: lte.Cell	Severity: critical Specific problem: CELL DISABLED DUE TO LRA Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell was disabled by a LRA from another alarm.		
Remedial action: Lock and unlock the cell. If the alarm persists. Call the next level of support. Check the Event Log for more details.		

Table 29-1494 IK4306017

Alarm	Attributes	Applicable major release
Name: IK4306017 (5364) Type: processingErrorAlarm Package: lte.IK4306017 Raised on class: lte.AntennaPort	Severity: warning Specific problem: PARAMETER WRITE FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: An antenna port parameter (such as antennaGainConfigure or horizontalBeamwidthConfigure) was set, however the corresponding parameter (antennaGain, horizontalBeamwidth) could not be changed, possibly because the value is read from the hardware (such as for AA units). The SAM and eNodeB databases have different values for these parameters while the alarm is raised.		
Remedial action: Determine the equipped RFM type. If AA, then antenna characteristics are read from the hardware and cannot be modified. Change the setting (antennaGainConfigure, horizontalBeamwidthConfigure, or other) back to Unset.		

Table 29-1495 IK4306022

Alarm	Attributes	Applicable major release
Name: IK4306022 (5000) Type: processingErrorAlarm Package: lte.IK4306022 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: IPSEC KEY GENERATION FAILURE Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNB platform failed to generate an RSA key pair for IPsec.		
Remedial action: Reboot the eNB manually at a later time. If this problem continues, the operator should contact the support.		

Table 29-1496 IK4306023

Alarm	Attributes	Applicable major release
Name: IK4306023 (5001) Type: processingErrorAlarm Package: lte.IK4306023 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: IPSEC IKE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm indicates IPSec IKE configuration failure.		
Remedial action: Check the correctness of the eNB configuration data and apply the data again. eNB should reset. If after eNB start-up the problem/alarm persists and the problem is not related to eNB misconfiguration then call next level of support.		

Table 29-1497 IK4306024

Alarm	Attributes	Applicable major release
Name: IK4306024 (5002) Type: equipmentAlarm Package: lte.IK4306024 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MEDO LOSS OF COMMUNICATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that a failure in internal communication with the Metro Dock.		
Remedial action: Check for connectivity with the board.		

Table 29-1498 IK4306025

Alarm	Attributes	Applicable major release
Name: IK4306025 (5003) Type: equipmentAlarm Package: lte.IK4306025 Raised on class: lte.Cell	Severity: critical Specific problem: HW SW CAPABILITY INCOMPATIBLE MODEM TYPE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the installed modem type is not compatible with installed controller board or with expectedModemType.		
Remedial action: The operator has to 1 - lock the cell. 2 - change the MIM configuration accordingly the installed eNB HW. 3 - unlock the cell.		

Table 29-1499 IK4306026

Alarm	Attributes	Applicable major release
Name: IK4306026 (5004) Type: equipmentAlarm Package: lte.IK4306026 Raised on class: lte.Cell	Severity: critical Specific problem: HW SW CAPABILITY EXPECTED CONTROLLER NOT EQUIPPED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the installed controller type is not compatible with the expectedControllerType in MIM.		
Remedial action: The operator has to 1 - lock the cell. 2 - change the MIM configuration accordingly the installed eNB controller HW. 3 - unlock the cell.		

Table 29-1500 IK4306027

Alarm	Attributes	Applicable major release
Name: IK4306027 (5005) Type: processingErrorAlarm Package: lte.IK4306027 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: UNEXPECTED BASEBAND BOARD RESET BB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the baseband board suffered from an unexpected, unplanned reset. \nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for the support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact the support for further assistance.		
Remedial action: No action is required.		

Table 29-1501 IK4306028

Alarm	Attributes	Applicable major release
Name: IK4306028 (5006) Type: qualityOfServiceAlarm Package: lte.IK4306028 Raised on class: lte.Cell	Severity: indeterminate Specific problem: INTER-FREQ LOAD BALANCING BEGIN Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicate that inter-freq load balancing procedure begins.		
Remedial action: No action is required.		

Table 29-1502 IK4306029

Alarm	Attributes	Applicable major release
Name: IK4306029 (5007) Type: qualityOfServiceAlarm Package: lte.IK4306029 Raised on class: lte.Cell	Severity: indeterminate Specific problem: INTER-FREQ LOAD BALANCING END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicate that inter-freq load balancing procedure ends.		
Remedial action: No action is required.		

Table 29-1503 IK4306030

Alarm	Attributes	Applicable major release
Name: IK4306030 (5008) Type: qualityOfServiceAlarm Package: lte.IK4306030 Raised on class: lte.Mce	Severity: indeterminate Specific problem: MCE CAC FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: Description1: MCE admission reaches the max nbr of sessions in MBSFN Area -MbsfnareaId-;. Failed sessions -listofFailedTmgi-; at time -TargetUtcTime-;\n\nDescription2: MCE admission reaches the max nbr of available sub-frames in MBSFN Area -MbsfnareaId- at time -TargetUtcTime-;. Nbr of needed Sf -; NbrNeededSf-;, nbr of available Sf -NbrAvailableSf-;, failed sessions -listofFailedTmgi-;		
Remedial action: No action is required.		

Table 29-1504 IK4306031

Alarm	Attributes	Applicable major release
Name: IK4306031 (5009) Type: processingErrorAlarm Package: lte.IK4306031 Raised on class: lte.Mce	Severity: indeterminate Specific problem: M2 ERROR INDICATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the fault is still present on eNB side in despite of a M2 ERROR INDICATION procedure previously exchanged between the eNB and the MCE to solve the issue.		
Remedial action: No action is required.		

Table 29-1505 IK4306032

Alarm	Attributes	Applicable major release
Name: IK4306032 (5010) Type: processingErrorAlarm Package: lte.IK4306032 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: PCI RAISED RECORD REMOVED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates SAM/operator that the raised PCI changing request is deleted by eNB itself due to the PCI status changing to unresolved or resolved by other ways.		
Remedial action: No action is required.		

Table 29-1506 IK4306033

Alarm	Attributes	Applicable major release
Name: IK4306033 (5011) Type: qualityOfServiceAlarm Package: lte.IK4306033 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: SON REQUEST TABLE NOT EMPTY Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates SAM/operator that there are valid SON 'changing request records' remaining and waiting for operator feedback in the SON control mode.		
Remedial action: Operator give feedback on the existing 'changing request record'.		

Table 29-1507 IK4306034

Alarm	Attributes	Applicable major release
Name: IK4306034 (5012) Type: qualityOfServiceAlarm Package: lte.IK4306034 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: SON REQUEST TABLE FULL Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates SAM/operator that there is no valid SON related 'changing request records' can be raised by eNB in the SON control mode.		
Remedial action: Operator give feedback on the existing request record.		

Table 29-1508 IK4306035

Alarm	Attributes	Applicable major release
Name: IK4306035 (5365) Type: communicationsAlarm Package: lte.IK4306035 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: INCONSISTENT IP VERSION MULTICAST ADDRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that inconsistency between the VLAN configuration in the eNB and the IP version of the multicast address or the IP version of the multicast source address received in the M3 Session Start and M2 Session Start messages.		
Remedial action: No action is required.		

Table 29-1509 IK4306036

Alarm	Attributes	Applicable major release
Name: IK4306036 (5366) Type: equipmentAlarm Package: lte.IK4306036 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM MODEM FUNCTION FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1510 IK4306038

Alarm	Attributes	Applicable major release
Name: IK4306038 (5368) Type: securityServiceOrMechanismViolation Package: lte.IK4306038 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DNS RESOLUTION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the searched item does not exist in DNS		
Remedial action: No action is required.		

Table 29-1511 IK4306039

Alarm	Attributes	Applicable major release
Name: IK4306039 (5369) Type: equipmentAlarm Package: lte.IK4306039 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: LOSS OF EMBMS PHASE SYNC Implicitly cleared: true Default probable cause: lossOfSignal	Release: • LR15.1.L

Table 29-1511 IK4306039 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the phase-sync requirement for supporting eMBMS can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1512 IK4306040

Alarm	Attributes	Applicable major release
Name: IK4306040 (5370) Type: processingErrorAlarm Package: lte.IK4306040 Raised on class: lte.Cell	Severity: indeterminate Specific problem: LOGICAL RESET AND RF RECONF DUE TO ON-LINE B-CELL+RF(s) CLASS PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the LTE Cell is logically reset and the RF is reconfigured during parameter update procedure.		
Remedial action: No action is required.		

Table 29-1513 IK4306041

Alarm	Attributes	Applicable major release
Name: IK4306041 (5371) Type: communicationsAlarm Package: lte.IK4306041 Raised on class: lte.Cell	Severity: warning Specific problem: SHUTDOWN TIMEOUT WITH EMERGENCY HIGH PRIORITY CALLS ACTIVE Implicitly cleared: true Default probable cause: callEstablishmentError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the shutdown timer has expired for a shutting down MO but the cell has at least one emergency or high priority call active. The shutting down MO will not be locked until all emergency and high priority calls have terminated.		
Remedial action: Operator should wait for all emergency and high priority calls to terminate or force the shut down to end by locking the shutting down MO.		

Table 29-1514 IK4306042

Alarm	Attributes	Applicable major release
Name: IK4306042 (5372) Type: communicationsAlarm Package: lte.IK4306042 Raised on class: lte.Cell	Severity: warning Specific problem: EMERGENCY HIGH PRIORITY CALLS ACTIVE FOR BLOCKED CELL Implicitly cleared: true Default probable cause: callEstablishmentError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that there is at least one emergency or high priority call active on a cell that is blocked. The cell will not be disabled until all emergency and high priority calls have terminated.		

Table 29-1514 IK4306042 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Operator should wait for all emergency and high priority calls to terminate or force the shut down to end by locking the shutting down MO.		

Table 29-1515 IK4306043

Alarm	Attributes	Applicable major release
Name: IK4306043 (5373) Type: equipmentAlarm Package: lte.IK4306043 Raised on class: lte.MODULE	Severity: critical Specific problem: WALG INITIALIZATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a failure to initialize the eNodeB network processor.		
Remedial action: Reset the eNodeB.		

Table 29-1516 IK4306044

Alarm	Attributes	Applicable major release
Name: IK4306044 (5013) Type: processingErrorAlarm Package: lte.IK4306044 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB UNEXPECTED PARTIAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned partial failure on the CB.\nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1517 IK4306045

Alarm	Attributes	Applicable major release
Name: IK4306045 (5014) Type: processingErrorAlarm Package: lte.IK4306045 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB UNEXPECTED PARTIAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1517 IK4306045 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the ENB suffered from an unexpected, unplanned partial failure on the BB.\nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1518 IK4306046

Alarm	Attributes	Applicable major release
Name: IK4306046 (5015) Type: processingErrorAlarm Package: lte.IK4306046 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB UNEXPECTED PARTIAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned partial failure on the SCB.\nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1519 IK4306048

Alarm	Attributes	Applicable major release
Name: IK4306048 (5017) Type: processingErrorAlarm Package: lte.IK4306048 Raised on class: lte.Cell	Severity: indeterminate Specific problem: MBMS RADIO CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the radio configuration made by the MCE for eMBMS could not be setup correctly.		
Remedial action: No action is required.		

Table 29-1520 IK4306050

Alarm	Attributes	Applicable major release
Name: IK4306050 (5019) Type: equipmentAlarm Package: lte.IK4306050 Raised on class: lte.Cell	Severity: major Specific problem: BAND CLASS-BANDWIDTH NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that when a non-supported Band Class or Bandwidth is detected based on the Metro modem type.		
Remedial action: 1 - Lock the cell. ; 2.Make sure to configure/equip the supported Band-class or Band width based on the equipped Modem type.; 3. -Unlock the cell.		

Table 29-1521 IK4306051

Alarm	Attributes	Applicable major release
Name: IK4306051 (5020) Type: equipmentAlarm Package: lte.IK4306051 Raised on class: lte.Cell	Severity: minor Specific problem: MODEM CAPACITY CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that if the capacity tolerance check fails based on the Metro modem type.		
Remedial action: Check the capacity tolerance based the equipped Modem type.		

Table 29-1522 IK4306052

Alarm	Attributes	Applicable major release
Name: IK4306052 (5021) Type: equipmentAlarm Package: lte.IK4306052 Raised on class: lte.MODULE	Severity: critical Specific problem: MODEM BOARD INCOMPATIBLE WITH CONTROLLER BOARD Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the modem board is not compatible with the controller board.		
Remedial action: Change the modem board to a modem board supported by the controller type.		

Table 29-1523 IK4306053

Alarm	Attributes	Applicable major release
Name: IK4306053 (5022) Type: processingErrorAlarm Package: lte.IK4306053 Raised on class: lte.CBCardSpecifics	Severity: warning Specific problem: CB DATA BASE RESTORE FAILURE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates if eNB fails to download successfully the full DB backup file for a full DB restore request, this alarm will be raised and the download will be failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1524 IK4306061

Alarm	Attributes	Applicable major release
Name: IK4306061 (5374) Type: equipmentAlarm Package: lte.IK4306061 Raised on class: lte.MODULE	Severity: major Specific problem: LOSS OF EMBMS PHASE SYNC Implicitly cleared: true Default probable cause: lossOfSignal	Release: • LR15.1.L
Description: This alarm indicates that the phase-sync requirement for supporting eMBMS can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1525 IK4306062

Alarm	Attributes	Applicable major release
Name: IK4306062 (5375) Type: processingErrorAlarm Package: lte.IK4306062 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB UNEXPECTED SOC FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned partial failure on a SOC of a CB. More detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1526 IK4306063

Alarm	Attributes	Applicable major release
Name: IK4306063 (5376) Type: processingErrorAlarm Package: lte.IK4306063 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB UNEXPECTED SOC FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned partial failure on a SOC of a BB.\nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1527 IK4306064

Alarm	Attributes	Applicable major release
Name: IK4306064 (5377) Type: equipmentAlarm Package: lte.IK4306064 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: ENB LOCATION VERIFICATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNB may not be in the expected location.		
Remedial action: Check the bbu Configured latitude and longitude and the bbuPositionErrorThreshold.		

Table 29-1528 IK4306065

Alarm	Attributes	Applicable major release
Name: IK4306065 (5378) Type: equipmentAlarm Package: lte.IK4306065 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: RET SOFTWARE DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to RET unit Started.		
Remedial action: No action is required.		

Table 29-1529 IK4306066

Alarm	Attributes	Applicable major release
Name: IK4306066 (5024) Type: processingErrorAlarm Package: lte.IK4306066 Raised on class: lte.RRH	Severity: minor Specific problem: CONFIGURED CELL RESOURCES MISMATCH VERSUS HARDWARE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the eNodeB configured cell resources versus the hardware capacity.		
Remedial action: Verify and correct the configuration data or Verify and correct the hardware configuration		

Table 29-1530 IK4306067

Alarm	Attributes	Applicable major release
Name: IK4306067 (5379) Type: equipmentAlarm Package: lte.IK4306067 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: RET SOFTWARE DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to a RET unit Completed. The RET unit will reset automatically and would start on the new software		
Remedial action: No action is required.		

Table 29-1531 IK4306068

Alarm	Attributes	Applicable major release
Name: IK4306068 (5380) Type: equipmentAlarm Package: lte.IK4306068 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: RET ACF DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a Download of an Antenna Configuration File to RET Subunit Started. The RET unit will not operational until the download is completed.		
Remedial action: No action is required.		

Table 29-1532 IK4306069

Alarm	Attributes	Applicable major release
Name: IK4306069 (5025) Type: qualityOfServiceAlarm Package: lte.IK4306069 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL RECONFIGURATION ATTEMPT TO A NEW BB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that an attempt to reconfigure the LteCell to a new BB is performed. This procedure happens when a BB meets a permanent failure or when a new BB is inserted in the DBU.		
Remedial action: No action is required.		

Table 29-1533 IK4306070

Alarm	Attributes	Applicable major release
Name: IK4306070 (5026) Type: equipmentAlarm Package: lte.IK4306070 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: LOSS OF ECSFB PHASE SYNC Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L
Description: This alarm indicates that the 10us phase-sync requirement for supporting eCSFB can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1534 IK4306077

Alarm	Attributes	Applicable major release
Name: IK4306077 (5027) Type: equipmentAlarm Package: lte.IK4306077 Raised on class: lte.MODULE	Severity: major Specific problem: LOSS OF ECSFB PHASE SYNC Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L
Description: This alarm indicates that the 10us phase-sync requirement for supporting eCSFB can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1535 IK4306079

Alarm	Attributes	Applicable major release
Name: IK4306079 (5029) Type: processingErrorAlarm Package: lte.IK4306079 Raised on class: lte.Cell	Severity: critical Specific problem: CELL RESET OAM TIMEOUT Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates message from eNB OAM is not received in Cellcallp in time		
Remedial action: Lock and unlock the cell. If the alarm persists. Call the next level of support.		

Table 29-1536 IK4306080

Alarm	Attributes	Applicable major release
Name: IK4306080 (5381) Type: equipmentAlarm Package: lte.IK4306080 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TMA SOFTWARE DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to TMA unit Started.		
Remedial action: No action is required.		

Table 29-1537 IK4306081

Alarm	Attributes	Applicable major release
Name: IK4306081 (5382) Type: equipmentAlarm Package: lte.IK4306081 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TMA SOFTWARE DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to a TMA unit Completed. The TMA unit will reset automatically and would start on the new software		
Remedial action: No action is required.		

Table 29-1538 IK4306082

Alarm	Attributes	Applicable major release
Name: IK4306082 (5383) Type: equipmentAlarm Package: lte.IK4306082 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: RET ACF DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the Download of the ACF to the RET unit completed.		
Remedial action: No action is required.		

Table 29-1539 IK4306092

Alarm	Attributes	Applicable major release
Name: IK4306092 (5030) Type: equipmentAlarm Package: lte.IK4306092 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODEM RESET DUE TO RE-ASSIGNMENT OF MODEM RESOURCES Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The event indicates that a Modem has been reset due to the re-assignment of the modem resources to cells.		
Remedial action: No action is required.		

Table 29-1540 IK4306093

Alarm	Attributes	Applicable major release
Name: IK4306093 (5031) Type: equipmentAlarm Package: lte.IK4306093 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE ONE LOGIC CELL NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the OLC feature is not supported by current cell configuration.		
Remedial action: Verify and correct the configuration data.		

Table 29-1541 IK4306094

Alarm	Attributes	Applicable major release
Name: IK4306094 (5032) Type: equipmentAlarm Package: lte.IK4306094 Raised on class: lte.Cell	Severity: critical Specific problem: FEATURE RRH DAISY CHAIN NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell mapped on chained RRH is not supported by equipped controller type.		
Remedial action: Verify and correct the configuration data.		

Table 29-1542 IK4306096

Alarm	Attributes	Applicable major release
Name: IK4306096 (5034) Type: operationalViolation Package: lte.IK4306096 Raised on class: lte.Cell	Severity: critical Specific problem: PCI UNSOLVED UNDER CONTROLLED MODE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates a PCI conflict (collision and/or confusion) between the cell and a neighbour one. A manual intervention is needed to solve the problem. This can happen in the following case: The recommended PCI value can't be raised by eNB and PCI controlled mode is activated.		
Remedial action: Increase the list of allowed PCI values, either for the local or for the distant eNodeB or manual PCI online modification from SAM.		

Table 29-1543 IK4306101

Alarm	Attributes	Applicable major release
Name: IK4306101 (5038) Type: communicationsAlarm Package: lte.IK4306101 Raised on class: lte.Cell	Severity: indeterminate Specific problem: PCI CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a new PCI is assigned by the eNodeB to the cell.		
Remedial action: No action is required.		

Table 29-1544 IK4306107

Alarm	Attributes	Applicable major release
Name: IK4306107 (5039) Type: equipmentAlarm Package: lte.IK4306107 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ALL ALARMS CLEARED Implicitly cleared: true Default probable cause: softwareProgramAbnormally-Terminated	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This is a pseudo alarm to indicate that all pending alarms have been cleared, e.g. by a reset of the eNB controller.		
Remedial action: No Maintenance Action required.		

Table 29-1545 IK4306116

Alarm	Attributes	Applicable major release
Name: IK4306116 (8013) Type: processingErrorAlarm Package: lte.IK4306116 Raised on class: lte.Cell	Severity: major Specific problem: SIM HEALTH CHECK PHASE 1 - TX PWR FAILED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB cell, has detected an active antenna transmit path (Cell, RFM id, antenna port #) with zero power continually for the Phase 1 detection period.		
Remedial action: No action is required. If the degradation persists, SIM may escalate to Local Recovery Action on the implicated cell.		

Table 29-1546 IK4306117

Alarm	Attributes	Applicable major release
Name: IK4306117 (8014) Type: processingErrorAlarm Package: lte.IK4306117 Raised on class: lte.Cell	Severity: major Specific problem: SIM HEALTH CHECK PHASE 1 - LOW RRC SUCCESS RATE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected a degradation in the RRC Success Rate on the cell. This is the SIM Phase 1 detection.		
Remedial action: No action is required. If the degradation persists, SIM may escalate to Local Recovery Action.		

Table 29-1547 IK4306118

Alarm	Attributes	Applicable major release
Name: IK4306118 (8015) Type: processingErrorAlarm Package: lte.IK4306118 Raised on class: lte.Cell	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 2 - LOW RRC SUCCESS RATE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the RRC Success Rate degradation has persisted beyond the configurable limit. This is the SIM Phase 2 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1548 IK4306119

Alarm	Attributes	Applicable major release
Name: IK4306119 (8016) Type: processingErrorAlarm Package: lte.IK4306119 Raised on class: lte.Cell	Severity: indeterminate Specific problem: SIM HEALTH CHECK - MAXIMUM NUMBER OF LRA REACHED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The OAM System Integrity Monitor has run a SIM Health Check on the cell and has detected a degradation that has escalated to the point of Phase 2 recovery. But, since SIM has already taken the configurable maximum number of SIM triggered Phase 2 recovery actions on this cell in a 24 hour period, SIM is prevented from taking recovery on this detection. Investigation is required to determine the cause for the frequent degradations.		
Remedial action: No action is required.		

Table 29-1549 IK4306120

Alarm	Attributes	Applicable major release
Name: IK4306120 (8017) Type: equipmentAlarm Package: lte.IK4306120 Raised on class: lte.RFME	Severity: indeterminate Specific problem: UNEXPECTED RFME MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the ENB suffered from an unexpected, unplanned failure on the RFME. Specific details are in the Additional Text.		
Remedial action: No action is required.		

Table 29-1550 IK4306121

Alarm	Attributes	Applicable major release
Name: IK4306121 (8018) Type: processingErrorAlarm Package: lte.IK4306121 Raised on class: lte.Cell	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 2 - TX PWR FAILED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected an active antenna transmit path (Cell, RFM id, antenna port #) with zero power continually for the Phase 2 detection period.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1551 IK4306122

Alarm	Attributes	Applicable major release
Name: IK4306122 (8019) Type: processingErrorAlarm Package: lte.IK4306122 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SMART COLLECTION SERVICE ACTION PLAN COMPLETE Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the Smart Collection Service initiated a smart data collection and has either 1) created a Local File, 2) streamed DDT to the DTC, and/or 3) used On Demand File Collection to push the ODFC archive to the Snapshots and Postmortem Collector entity (SPC). This was triggered by a fault event or state change. Specific details about the triggering event and the files that were collected are in the Additional Text.		
Remedial action: No action is required.		

Table 29-1552 IK4306123

Alarm	Attributes	Applicable major release
Name: IK4306123 (8020) Type: qualityOfServiceAlarm Package: lte.IK4306123 Raised on class: lte.Cell	Severity: warning Specific problem: HANDOVER OPTIMIZATION ADJUSTMENT STARTED Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the SON process that adjusts intra-frequency handover parameters has started adjusting handover parameters.		
Remedial action: No action is required. This alarm is provided to allow operator to correlate handover optimization adjustment with other issues that may happen in the network at the same time.		

Table 29-1553 IK4306126

Alarm	Attributes	Applicable major release
Name: IK4306126 (8022) Type: processingErrorAlarm Package: lte.IK4306126 Raised on class: lte.RFM	Severity: major Specific problem: RFM CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates the failure to configure the RFM.		
Remedial action: Reset the module. If the alarm persists, replace the module.		

Table 29-1554 IK4306127

Alarm	Attributes	Applicable major release
Name: IK4306127 (8794) Type: processingErrorAlarm Package: lte.IK4306127 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TARGET OBJECT IS UNREACHABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt to send a command by the operator to a TMA failed.		
Remedial action: No action is required.		

Table 29-1555 IK4306128

Alarm	Attributes	Applicable major release
Name: IK4306128 (8795) Type: processingErrorAlarm Package: lte.IK4306128 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: TARGET OBJECT IS UNREACHABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt to send a command by the operator to a RET unit failed.		
Remedial action: No action is required.		

Table 29-1556 IK4306129

Alarm	Attributes	Applicable major release
Name: IK4306129 (8796) Type: processingErrorAlarm Package: lte.IK4306129 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: AISG COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt to send a command by the operator to a TMA unit failed.		

Table 29-1556 IK4306129 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1557 IK4306130

Alarm	Attributes	Applicable major release
Name: IK4306130 (8797) Type: processingErrorAlarm Package: lte.IK4306130 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: AISG COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt to send a command by the operator to a RET unit failed.		
Remedial action: No action is required.		

Table 29-1558 IK4306131

Alarm	Attributes	Applicable major release
Name: IK4306131 (10134) Type: processingErrorAlarm Package: lte.IK4306131 Raised on class: lte.RFM	Severity: indeterminate Specific problem: NO NEW DEVICE FOUND AFTER RUN AISG SCAN Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the RFM did not discover any additional ALD (RET or TMA or MTS or RAE) on the AISG after it completed the AISG Scan command.		
Remedial action: If the Operator believes that there are ALDs on the RFM, the command should be repeated. If the command does not return any new ALDs, the operator might have to send some to the site to check the AISG cable connections.		

Table 29-1559 IK4306132

Alarm	Attributes	Applicable major release
Name: IK4306132 (8798) Type: processingErrorAlarm Package: lte.IK4306132 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: SET DEVICE DATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt by the operator to write to one of the additional data record failed.		
Remedial action: No action is required.		

Table 29-1560 IK4306133

Alarm	Attributes	Applicable major release
Name: IK4306133 (8799) Type: processingErrorAlarm Package: lte.IK4306133 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: SET DEVICE DATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt by the operator to write to one of the additional data record failed.		
Remedial action: No action is required.		

Table 29-1561 IK4306134

Alarm	Attributes	Applicable major release
Name: IK4306134 (8800) Type: processingErrorAlarm Package: lte.IK4306134 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: PERIODIC ANTENNA TILT CHECK NOT DONE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB OMA was not able to check the antenna electrical tilt of a RET Subunit.		
Remedial action: No action is required.		

Table 29-1562 IK4306135

Alarm	Attributes	Applicable major release
Name: IK4306135 (8801) Type: equipmentAlarm Package: lte.IK4306135 Raised on class: lte.RRH	Severity: minor Specific problem: RRH NOT ALLOWED BY ENB TYPE LICENSE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the licence for the eNB type does not allow this RRH. The performance of this RRH goes beyond what the licence for the eNB type allows.		
Remedial action: No action is required. The operator has to use another and appropriate RRH.		

Table 29-1563 IK4306136

Alarm	Attributes	Applicable major release
Name: IK4306136 (8802) Type: equipmentAlarm Package: lte.IK4306136 Raised on class: lte.TRDU	Severity: minor Specific problem: TRDU NOT ALLOWED BY ENB TYPE LICENSE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the licence for the eNB type does not allow this TRDU. The performance of this TRDU goes beyond what the licence for the eNB type allows		
Remedial action: No action is required. The operator has to use another and appropriate TRDU.		

Table 29-1564 IK4306137

Alarm	Attributes	Applicable major release
Name: IK4306137 (8803) Type: equipmentAlarm Package: lte.IK4306137 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MODEM NOT ALLOWED BY ENB TYPE LICENSE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the licence for the eNB type does not allow this modem. The performance of this modem goes beyond what the licence for the eNB type allows.		
Remedial action: No action is required. The operator has to use another and appropriate modem.		

Table 29-1565 IK4306138

Alarm	Attributes	Applicable major release
Name: IK4306138 (8804) Type: equipmentAlarm Package: lte.IK4306138 Raised on class: lte.RRH	Severity: minor Specific problem: RFM CONTROL MODE ERROR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is used for: Incompatible RFM with Controller Mode.		
Remedial action: Reconfigure the RE to correct the value of any parameter described in the alarm additional information.		

Table 29-1566 IK4306139

Alarm	Attributes	Applicable major release
Name: IK4306139 (8805) Type: equipmentAlarm Package: lte.IK4306139 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP EXCESS TEST SESSION REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates 6 TWAMP test-sessions have been requested in a TWAMP Control-session in a VLAN. 5 is the maximum supported number.\n\nCheck TWAMP client configuration to ensure it matches maximum requirements of the base station server.		
Remedial action: No action is required.		

Table 29-1567 IK4306140

Alarm	Attributes	Applicable major release
Name: IK4306140 (8806) Type: equipmentAlarm Package: lte.IK4306140 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP EXCESS CONTROL SESSION REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates 5 TWAMP Control sessions have been requested in a VLAN. 4 is the maximum supported number.\n\nCheck TWAMP client configuration to ensure it matches maximum requirements of the base station server.		
Remedial action: No action is required.		

Table 29-1568 IK4306141

Alarm	Attributes	Applicable major release
Name: IK4306141 (8807) Type: equipmentAlarm Package: lte.IK4306141 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP TEST SESSION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: A TWAMP session in the VLAN has failed based on lack of incoming Test packets for a period of time configured by SERVWAIT/REFWAIT timers.\n\nCheck TWAMP client and the backhaul link between TWAMP client and base station for any backhaul connectivity failure.		
Remedial action: No action is required.		

Table 29-1569 IK4306142

Alarm	Attributes	Applicable major release
Name: IK4306142 (8808) Type: equipmentAlarm Package: lte.IK4306142 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP MODE MISMATCH Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The server has a TWAMP Control session Request with an unacceptable Mode value. Only 'Unauthenticated' is acceptable.\n\nCheck TWAMP client configuration to ensure it matches the acceptable 'mode' value for Unauthentication.		
Remedial action: No action is required.		

Table 29-1570 IK4306143

Alarm	Attributes	Applicable major release
Name: IK4306143 (8809) Type: processingErrorAlarm Package: lte.IK4306143 Raised on class: lte.Cell	Severity: indeterminate Specific problem: SIM LOCAL RECOVERY ACTION - CELL Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The OAM System Integrity Monitor has run a Health Check on the cell and has detected a degradation affecting cell performance. SIM has raised a critical alarm and is now initiating Phase 2 recovery actions to initialize the Cell.		
Remedial action: No action is required.		

Table 29-1571 IK4306144

Alarm	Attributes	Applicable major release
Name: IK4306144 (8810) Type: processingErrorAlarm Package: lte.IK4306144 Raised on class: lte.RFM	Severity: indeterminate Specific problem: SIM LOCAL RECOVERY ACTION - RFM Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: The OAM System Integrity Monitor has run a Health Check on the cell and has detected a degradation affecting cell performance. SIM has raised a critical alarm and is now initiating Phase 3 recovery actions to initialize the RFM.		
Remedial action: No action is required.		

Table 29-1572 IK4306145

Alarm	Attributes	Applicable major release
Name: IK4306145 (8811) Type: processingErrorAlarm Package: lte.IK4306145 Raised on class: lte.Cell	Severity: major Specific problem: SIM HEALTH CHECK PHASE 1 - CELL OUTAGE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected a zero RRC attempt rate on the cell. This is the SIM Phase 1 detection.		
Remedial action: No action is required. If the degradation persists, SIM may escalate to Local Recovery Action.		

Table 29-1573 IK4306146

Alarm	Attributes	Applicable major release
Name: IK4306146 (8812) Type: processingErrorAlarm Package: lte.IK4306146 Raised on class: lte.Cell	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 2 - CELL OUTAGE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the zero RRC attempt rate has persisted beyond the configurable limit. This is the SIM Phase 2 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1574 IK4306147

Alarm	Attributes	Applicable major release
Name: IK4306147 (8813) Type: processingErrorAlarm Package: lte.IK4306147 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TROUBLESHOOTING WATCHDOG - TOOL START Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: The Troubleshooting Watchdog has detected that a troubleshooting tool has been started. The additional info provides information about the troubleshooting tool invocation.		
Remedial action: No action is required.		

Table 29-1575 IK4306148

Alarm	Attributes	Applicable major release
Name: IK4306148 (8814) Type: processingErrorAlarm Package: lte.IK4306148 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TROUBLESHOOTING WATCHDOG - TOOL STOP Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: The Troubleshooting Watchdog has detected that a troubleshooting tool has been stopped. The additional info provides information about the troubleshooting tool and any watchdog actions taken to stop the tool.		
Remedial action: No action is required.		

Table 29-1576 IK4306149

Alarm	Attributes	Applicable major release
Name: IK4306149 (8815) Type: equipmentAlarm Package: lte.IK4306149 Raised on class: lte.MODULE	Severity: minor Specific problem: OAM MODEM FUNCTION FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1577 IK4306150

Alarm	Attributes	Applicable major release
Name: IK4306150 (8816) Type: equipmentAlarm Package: lte.IK4306150 Raised on class: lte.MODULE	Severity: major Specific problem: OAM MODEM FUNCTION FAULT 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1578 IK4306151

Alarm	Attributes	Applicable major release
Name: IK4306151 (8817) Type: processingErrorAlarm Package: lte.IK4306151 Raised on class: lte.Rae	Severity: indeterminate Specific problem: AISG COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1578 IK4306151 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the attempt to send a command by the operator to a RAE unit failed.		
Remedial action: No action is required.		

Table 29-1579 IK4306152

Alarm	Attributes	Applicable major release
Name: IK4306152 (8818) Type: processingErrorAlarm Package: lte.IK4306152 Raised on class: lte.Rae	Severity: indeterminate Specific problem: SET DEVICE DATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by the operator to write to one of the additional data record failed.		
Remedial action: No action is required.		

Table 29-1580 IK4306153

Alarm	Attributes	Applicable major release
Name: IK4306153 (8819) Type: processingErrorAlarm Package: lte.IK4306153 Raised on class: lte.Rae	Severity: indeterminate Specific problem: PERIODIC ANTENNA TILT CHECK NOT DONE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNodeB OMA was not able to check the antenna electrical tilt of a RAE Subunit.		
Remedial action: No action is required.		

Table 29-1581 IK4306154

Alarm	Attributes	Applicable major release
Name: IK4306154 (8820) Type: processingErrorAlarm Package: lte.IK4306154 Raised on class: lte.Rae	Severity: minor Specific problem: RAE SOFTWARE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the software download to the RAE unit failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1582 IK4306155

Alarm	Attributes	Applicable major release
Name: IK4306155 (8821) Type: processingErrorAlarm Package: lte.IK4306155 Raised on class: lte.Rae	Severity: minor Specific problem: RAESUBUNIT 1 ANTENNA CONFIGURATION FILE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the configuration file download to the RAESUBUNIT 1 failed.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1583 IK4306163

Alarm	Attributes	Applicable major release
Name: IK4306163 (8822) Type: equipmentAlarm Package: lte.IK4306163 Raised on class: lte.Rae	Severity: indeterminate Specific problem: RAE SOFTWARE DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to a RAE unit Started.		
Remedial action: No action is required.		

Table 29-1584 IK4306164

Alarm	Attributes	Applicable major release
Name: IK4306164 (8823) Type: equipmentAlarm Package: lte.IK4306164 Raised on class: lte.Rae	Severity: indeterminate Specific problem: RAE SOFTWARE DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a Software Download to a RAE unit Completed. The RAE unit will reset automatically and would start on the new software		
Remedial action: No action is required.		

Table 29-1585 IK4306165

Alarm	Attributes	Applicable major release
Name: IK4306165 (8824) Type: processingErrorAlarm Package: lte.IK4306165 Raised on class: lte.Rae	Severity: indeterminate Specific problem: READ DEVICE DATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by the eNodeB OAM to read from one of the additional data record failed.		
Remedial action: None		

Table 29-1586 IK4306166

Alarm	Attributes	Applicable major release
Name: IK4306166 (8825) Type: equipmentAlarm Package: lte.IK4306166 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OAM ENB FAULT 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: Provisioned for late churn-in.		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1587 IK4306169

Alarm	Attributes	Applicable major release
Name: IK4306169 (8826) Type: processingErrorAlarm Package: lte.IK4306169 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: CFG CHANGE NOT ACTIVATED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm indicates that configured local access state (from DB) has not been activated yet.		
Remedial action: Reset eNB to activate the configured local access state.		

Table 29-1588 IK4306170

Alarm	Attributes	Applicable major release
Name: IK4306170 (8827) Type: processingErrorAlarm Package: lte.IK4306170 Raised on classes: • lte.RFME • lte.AntennaPort • lte.TRDU • lte.RRH	Severity: warning Specific problem: CONFIGURATION DATA MISMATCH Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates inconsistency in the eNodeB configuration data versus the equipped hardware.		
Remedial action: Verify and correct the configuration data. Verify and correct the hardware configuration		

Table 29-1589 IK4306171

Alarm	Attributes	Applicable major release
Name: IK4306171 (8828) Type: processingErrorAlarm Package: lte.IK4306171 Raised on class: lte.MODULE	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the impacted module. If the alarm persists, contact the next level of support.		

Table 29-1590 IK4306172

Alarm	Attributes	Applicable major release
Name: IK4306172 (8829) Type: processingErrorAlarm Package: lte.IK4306172 Raised on class: lte.RFME	Severity: critical Specific problem: SW DOWNLOAD/ACTIVATION FAILURE Implicitly cleared: true Default probable cause: softwareError	Release: • LR15.1.L
Description: This alarm indicates a failure to download or activate the software for the new module.		
Remedial action: Reset the eNodeB. If the alarm persists, replace the module.		

Table 29-1591 IK4306173

Alarm	Attributes	Applicable major release
Name: IK4306173 (8830) Type: processingErrorAlarm Package: lte.IK4306173 Raised on class: lte.RFME	Severity: indeterminate Specific problem: SIM LOCAL RECOVERY ACTION - RFME Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: The OAM System Integrity Monitor has run a Health Check on the cell and has detected a degradation affecting cell performance. SIM has raised a critical alarm and is now initiating Phase 3 recovery actions to initialize the RFME.		
Remedial action: No action is required.		

Table 29-1592 IK4306174

Alarm	Attributes	Applicable major release
Name: IK4306174 (8831) Type: processingErrorAlarm Package: lte.IK4306174 Raised on class: lte.RFM	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - CELL OUTAGE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the zero RRC attempt rate has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1593 IK4306175

Alarm	Attributes	Applicable major release
Name: IK4306175 (8832) Type: processingErrorAlarm Package: lte.IK4306175 Raised on class: lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - CELL OUTAGE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the zero RRC attempt rate has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1594 IK4306176

Alarm	Attributes	Applicable major release
Name: IK4306176 (8833) Type: processingErrorAlarm Package: lte.IK4306176 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - TX PWR FAILED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected an active antenna transmit path (Cell, RFM id, antenna port #) with zero power continually for the Phase 3 detection period.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1595 IK4306177

Alarm	Attributes	Applicable major release
Name: IK4306177 (8834) Type: processingErrorAlarm Package: lte.IK4306177 Raised on class: lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - TX PWR FAILED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected an active antenna transmit path (Cell, RFM id, antenna port #) with zero power continually for the Phase 3 detection period.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1596 IK4306178

Alarm	Attributes	Applicable major release
Name: IK4306178 (8835) Type: processingErrorAlarm Package: lte.IK4306178 Raised on classes: • lte.RFM • lte.RetAldEntry • lte.Rae • lte.TmaAldEntry	Severity: minor Specific problem: SOFTWARE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The download of a new software application to the Hardware Failed. The hardware operation might not be possible.		
Remedial action: Retry the download. If the problem persists, contact the next level support.		

Table 29-1597 IK4306179

Alarm	Attributes	Applicable major release
Name: IK4306179 (8836) Type: processingErrorAlarm Package: lte.IK4306179 Raised on class: lte.RFM	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - LOW RRC SUCCESS RATE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the RRC Success Rate degradation has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1598 IK4306180

Alarm	Attributes	Applicable major release
Name: IK4306180 (8837) Type: processingErrorAlarm Package: lte.IK4306180 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: UNEXPECTED PARTIAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the system suffered from an unexpected, unplanned partial failure of a board. Specific details are in the Additional Text.		
Remedial action: No action is required.		

Table 29-1599 IK4306181

Alarm	Attributes	Applicable major release
Name: IK4306181 (8838) Type: processingErrorAlarm Package: lte.IK4306181 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: indeterminate Specific problem: UNEXPECTED SOC FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the system suffered from an unexpected, unplanned reset of a SOC on the alarmed board. Specific details are in the Additional Text.		
Remedial action: No action is required.		

Table 29-1600 IK4306182

Alarm	Attributes	Applicable major release
Name: IK4306182 (8839) Type: processingErrorAlarm Package: lte.IK4306182 Raised on class: lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - LOW RRC SUCCESS RATE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the RRC Success Rate degradation has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1601 IK4306183

Alarm	Attributes	Applicable major release
Name: IK4306183 (8840) Type: equipmentAlarm Package: lte.IK4306183 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: GNSS MODE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L
Description: This alarm indicates that the eNB does not support Glonass or GPS+Glonass mode. It only supports GPS mode		
Remedial action: Change the configuration of the eNB by configuring the GPS mode.		

Table 29-1602 IK4306184

Alarm	Attributes	Applicable major release
Name: IK4306184 (8841) Type: communicationsAlarm Package: lte.IK4306184 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: LONG ACTION COMPLETE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The OAM subsystem received a Netconf Long Action request from the EMS and now has completed it. This event notifies the SAM and documents the completion of a Netconf Long Action.		
Remedial action: No action is required.		

Table 29-1603 IK4306185

Alarm	Attributes	Applicable major release
Name: IK4306185 (8842) Type: qualityOfServiceAlarm Package: lte.IK4306185 Raised on class: lte.Cell	Severity: major Specific problem: ZERO ABS % Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: One or more macro NR cells is either setting its ABS % to 0 or is not communicating its ABS %.association for the SCo1 interface is down.		
Remedial action: Check if dynamic eICIC is enabled on the macro NR cells. Check if the X2 link(s) to the macro NR(s) are down.		

Table 29-1604 IK4306186

Alarm	Attributes	Applicable major release
Name: IK4306186 (8843) Type: communicationsAlarm Package: lte.IK4306186 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: NEW CERTIFICATE ACTIVATED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that operator certificate enrollment scenario started.		
Remedial action: No action is required.		

Table 29-1605 IK4306187

Alarm	Attributes	Applicable major release
Name: IK4306187 (8844) Type: equipmentAlarm Package: lte.IK4306187 Raised on class: lte.RRH	Severity: minor Specific problem: ANTENNA PORT RX PIM THRESH 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Passive Inter-Modulation detection minor alarm is indication of non-linearity in the antenna system. This may be caused by damage to the RF feeders, the antenna assembly or caused from external structures. Damage may be caused by water intrusion, crimped coaxial cables, loose connectors, lightning damage, or physical damage to the antenna assembly.		
Remedial action: Check for damage to the cable between the cabling between Radio Module output and/or damage to the physical antenna assembly. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. A survey of other external PIM sources might be performed.		

Table 29-1606 IK4306188

Alarm	Attributes	Applicable major release
Name: IK4306188 (8845) Type: equipmentAlarm Package: lte.IK4306188 Raised on class: lte.RRH	Severity: major Specific problem: ANTENNA PORT RX PIM THRESH 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: PIM detection urgent alarm is indication of non-linearity in the antenna system. This may be caused by damage to the RF feeders, the antenna assembly or caused from external structures. Damage may be caused by water intrusion, crimped coaxial cables, loose connectors, lightning damage, or physical damage to the antenna assembly.		
Remedial action: Check for damage to the cable between the cabling between Radio Module output and/or damage to the physical antenna assembly. Check the connection torque value between the Radio Module and the bulkhead. If the alarm persists then reset the RFM (Macro eNB) or in case of Metro all-in-one equipment reset eNB (Metro eNB) at the next maintenance window. A survey of other external PIM sources might be performed.		

Table 29-1607 IK4306189

Alarm	Attributes	Applicable major release
Name: IK4306189 (8846) Type: processingErrorAlarm Package: lte.IK4306189 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: GETDEVICEDATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt by OAM to read one of the additional data record failed.		
Remedial action: None.		

Table 29-1608 IK4306190

Alarm	Attributes	Applicable major release
Name: IK4306190 (8847) Type: processingErrorAlarm Package: lte.IK4306190 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: GETDEVICEDATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indiates that the attempt by OAM to read one of the additional data record failed.		
Remedial action: None.		

Table 29-1609 IK4306191

Alarm	Attributes	Applicable major release
Name: IK4306191 (8848) Type: processingErrorAlarm Package: lte.IK4306191 Raised on class: lte.Rae	Severity: indeterminate Specific problem: GETDEVICEDATA COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the attempt by OAM to read one of the additional data record failed.		
Remedial action: None.		

Table 29-1610 IK4306192

Alarm	Attributes	Applicable major release
Name: IK4306192 (8849) Type: processingErrorAlarm Package: lte.IK4306192 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CMS ENROLLMENT BEFORE OAM FAILED (ERROR) Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that eNB tried to enroll with the Operator PKI before the establishment of the end-to-end OAM connectivity but the procedure failed due to an error.		
Remedial action: Check the Sub CMS configuration. Verify and correct the CMS configuration data based on the error code received. Check the network connection. eNB has to get the initial operator-signed certificate(s) using the "enrollment before OAM" procedure before the end-to-end OAM connectivity can be setup.		

Table 29-1611 IK4306193

Alarm	Attributes	Applicable major release
Name: IK4306193 (8850) Type: processingErrorAlarm Package: lte.IK4306193 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CMS ENROLLMENT BEFORE OAM FAILED (TIMEOUT OR ENROLLMENT DATA ERROR) Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that eNB tried to enroll with the Operator PKI before the establishment of the end-to-end OAM connectivity but the procedure failed due to a timeout or a failure to initialize all CMS parameter values.		
Remedial action: No action is required.		

Table 29-1612 IK4306194

Alarm	Attributes	Applicable major release
Name: IK4306194 (8851) Type: processingErrorAlarm Package: lte.IK4306194 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: NEW CERTIFICATE PENDING FOR ACTIVATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a new certificate is pending for activation.		
Remedial action: No action is required.		

Table 29-1613 IK4306195

Alarm	Attributes	Applicable major release
Name: IK4306195 (8852) Type: processingErrorAlarm Package: lte.IK4306195 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: Transient IPsec interruption for certificate activation Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a new certificate is being activated. The protected traffic is interrupted.		
Remedial action: No action is required.		

Table 29-1614 IK4306196

Alarm	Attributes	Applicable major release
Name: IK4306196 (8853) Type: processingErrorAlarm Package: lte.IK4306196 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: CERTIFICATE ABOUT TO EXPIRE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The operator has to ensure that the certificate is renewed and activated.		
Remedial action: Force certificate enrollment and certificate activation if necessary.		

Table 29-1615 IK4306197

Alarm	Attributes	Applicable major release
Name: IK4306197 (8854) Type: processingErrorAlarm Package: lte.IK4306197 Raised on class: lte.ENBEquipment	Severity: major Specific problem: TELECOM SERVICE BLOCKED BY CERTIFICATE ENROLLMENT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The Telecom Service is blocked until the operator certificate is issued to eNB.		
Remedial action: Monitor the procedure for certificate enrollment.		

Table 29-1616 IK4306198

Alarm	Attributes	Applicable major release
Name: IK4306198 (8855) Type: equipmentAlarm Package: lte.IK4306198 Raised on classes: • lte.BBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: MODULE WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates an operator triggered warm reset of the managed object.		
Remedial action: No action is required.		

Table 29-1617 IK4306199

Alarm	Attributes	Applicable major release
Name: IK4306199 (8856) Type: equipmentAlarm Package: lte.IK4306199 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: UNEXPECTED CONTROL BOARD RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the control board suffered from an unexpected, unplanned reset. Specific details are in the Additional Text.		
Remedial action: No action is required.		

Table 29-1618 IK4306202

Alarm	Attributes	Applicable major release
Name: IK4306202 (8857) Type: equipmentAlarm Package: lte.IK4306202 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: LOSS OF ECSFB PHASE SYNC Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the 10us phase-sync requirement for supporting eCSFB can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1619 IK4306203

Alarm	Attributes	Applicable major release
Name: IK4306203 (8858) Type: equipmentAlarm Package: lte.IK4306203 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: indeterminate Specific problem: SOFTWARE DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a Software Download to the managed object completed. The unit will reset automatically and restarts on the new software.		
Remedial action: No action is required.		

Table 29-1620 IK4306204

Alarm	Attributes	Applicable major release
Name: IK4306204 (8859) Type: equipmentAlarm Package: lte.IK4306204 Raised on classes: • lte.RetAldEntry • lte.Rae • lte.TmaAldEntry	Severity: indeterminate Specific problem: SOFTWARE DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a Software Download to the managed unit started.		
Remedial action: No action is required.		

Table 29-1621 IK4306205

Alarm	Attributes	Applicable major release
Name: IK4306205 (8860) Type: equipmentAlarm Package: lte.IK4306205 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: LOSS OF EMBMS PHASE SYNC Implicitly cleared: true Default probable cause: lossOfSignal	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the phase-sync requirement for supporting eMBMS can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1622 IK4306206

Alarm	Attributes	Applicable major release
Name: IK4306206 (8861) Type: equipmentAlarm Package: lte.IK4306206 Raised on classes: • lte.RFM • lte.RFME	Severity: minor Specific problem: LOCAL CELL POWER LIMIT EXCEEDED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The downlink total power for a cell assigned to this RE exceeds the Local Cell Power Limit set at installation time.		
Remedial action: Reconfigure the cell of this RE: set the power to be less than or equal to the local cell power limit defined for this MSRE at installation time.		

Table 29-1623 IK4306207

Alarm	Attributes	Applicable major release
Name: IK4306207 (8862) Type: equipmentAlarm Package: lte.IK4306207 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: TOTAL LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eICIC functionality is being disabled due to very large clock drift		
Remedial action: Check the timing source of the eNB		

Table 29-1624 IK4306208

Alarm	Attributes	Applicable major release
Name: IK4306208 (8863) Type: equipmentAlarm Package: lte.IK4306208 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: minor Specific problem: LOSS OF EICIC PHASE SYNC Implicitly cleared: true Default probable cause: timingProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eICIC functionality is limited due to clock drift.		
Remedial action: No action is required.		

Table 29-1625 IK4306209

Alarm	Attributes	Applicable major release
Name: IK4306209 (8864) Type: equipmentAlarm Package: lte.IK4306209 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: critical Specific problem: END OF THE HOLDOVER DURATION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that when it is close to the end of the holdover duration of the internal oscillator		
Remedial action: No action is required.		

Table 29-1626 IK4306210

Alarm	Attributes	Applicable major release
Name: IK4306210 (8865) Type: equipmentAlarm Package: lte.IK4306210 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: No action is required.		

Table 29-1627 IK4306211

Alarm	Attributes	Applicable major release
Name: IK4306211 (8866) Type: equipmentAlarm Package: lte.IK4306211 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for MEDO for future use.		
Remedial action: No action is required.		

Table 29-1628 IK4306212

Alarm	Attributes	Applicable major release
Name: IK4306212 (8867) Type: equipmentAlarm Package: lte.IK4306212 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MEDO EVENT 3 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for MEDO for future use.		
Remedial action: No action is required.		

Table 29-1629 IK4306213

Alarm	Attributes	Applicable major release
Name: IK4306213 (8868) Type: equipmentAlarm Package: lte.IK4306213 Raised on class: lte.ENBEquipment	Severity: major Specific problem: MEDO FAULT 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for MEDO for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1630 IK4306214

Alarm	Attributes	Applicable major release
Name: IK4306214 (8869) Type: equipmentAlarm Package: lte.IK4306214 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: LOSS OF GEO LOC PHASE SYNC Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1630 IK4306214 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates loss of GPS high accuracy phase lock used for OTDOA.		
Remedial action: Check for proper GPS antenna placement.		

Table 29-1631 IK4306215

Alarm	Attributes	Applicable major release
Name: IK4306215 (8870) Type: equipmentAlarm Package: lte.IK4306215 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1632 IK4306216

Alarm	Attributes	Applicable major release
Name: IK4306216 (8871) Type: equipmentAlarm Package: lte.IK4306216 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1633 IK4306217

Alarm	Attributes	Applicable major release
Name: IK4306217 (8872) Type: equipmentAlarm Package: lte.IK4306217 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1634 IK4306218

Alarm	Attributes	Applicable major release
Name: IK4306218 (8873) Type: equipmentAlarm Package: lte.IK4306218 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1635 IK4306219

Alarm	Attributes	Applicable major release
Name: IK4306219 (8874) Type: equipmentAlarm Package: lte.IK4306219 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1636 IK4306220

Alarm	Attributes	Applicable major release
Name: IK4306220 (8875) Type: equipmentAlarm Package: lte.IK4306220 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1637 IK4306221

Alarm	Attributes	Applicable major release
Name: IK4306221 (8876) Type: equipmentAlarm Package: lte.IK4306221 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1637 IK4306221 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1638 IK4306222

Alarm	Attributes	Applicable major release
Name: IK4306222 (8877) Type: equipmentAlarm Package: lte.IK4306222 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1639 IK4306223

Alarm	Attributes	Applicable major release
Name: IK4306223 (8878) Type: equipmentAlarm Package: lte.IK4306223 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1640 IK4306224

Alarm	Attributes	Applicable major release
Name: IK4306224 (8879) Type: equipmentAlarm Package: lte.IK4306224 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1641 IK4306225

Alarm	Attributes	Applicable major release
Name: IK4306225 (8880) Type: equipmentAlarm Package: lte.IK4306225 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1642 IK4306226

Alarm	Attributes	Applicable major release
Name: IK4306226 (8881) Type: equipmentAlarm Package: lte.IK4306226 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1643 IK4306227

Alarm	Attributes	Applicable major release
Name: IK4306227 (8882) Type: equipmentAlarm Package: lte.IK4306227 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1644 IK4306228

Alarm	Attributes	Applicable major release
Name: IK4306228 (8883) Type: equipmentAlarm Package: lte.IK4306228 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1644 IK4306228 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1645 IK4306229

Alarm	Attributes	Applicable major release
Name: IK4306229 (8884) Type: equipmentAlarm Package: lte.IK4306229 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1646 IK4306230

Alarm	Attributes	Applicable major release
Name: IK4306230 (8885) Type: equipmentAlarm Package: lte.IK4306230 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1647 IK4306231

Alarm	Attributes	Applicable major release
Name: IK4306231 (8886) Type: equipmentAlarm Package: lte.IK4306231 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1648 IK4306232

Alarm	Attributes	Applicable major release
Name: IK4306232 (8887) Type: equipmentAlarm Package: lte.IK4306232 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1649 IK4306233

Alarm	Attributes	Applicable major release
Name: IK4306233 (8888) Type: equipmentAlarm Package: lte.IK4306233 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 11 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1650 IK4306234

Alarm	Attributes	Applicable major release
Name: IK4306234 (8889) Type: equipmentAlarm Package: lte.IK4306234 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 12 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1651 IK4306235

Alarm	Attributes	Applicable major release
Name: IK4306235 (8890) Type: equipmentAlarm Package: lte.IK4306235 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 13 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1651 IK4306235 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1652 IK4306236

Alarm	Attributes	Applicable major release
Name: IK4306236 (8891) Type: equipmentAlarm Package: lte.IK4306236 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 14 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1653 IK4306237

Alarm	Attributes	Applicable major release
Name: IK4306237 (8892) Type: equipmentAlarm Package: lte.IK4306237 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 15 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1654 IK4306238

Alarm	Attributes	Applicable major release
Name: IK4306238 (8893) Type: equipmentAlarm Package: lte.IK4306238 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 16 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1655 IK4306239

Alarm	Attributes	Applicable major release
Name: IK4306239 (8894) Type: equipmentAlarm Package: lte.IK4306239 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 17 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1656 IK4306240

Alarm	Attributes	Applicable major release
Name: IK4306240 (8895) Type: equipmentAlarm Package: lte.IK4306240 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 18 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1657 IK4306241

Alarm	Attributes	Applicable major release
Name: IK4306241 (8896) Type: equipmentAlarm Package: lte.IK4306241 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 19 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1658 IK4306242

Alarm	Attributes	Applicable major release
Name: IK4306242 (8897) Type: equipmentAlarm Package: lte.IK4306242 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 20 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1658 IK4306242 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1659 IK4306243

Alarm	Attributes	Applicable major release
Name: IK4306243 (8898) Type: equipmentAlarm Package: lte.IK4306243 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 21 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1660 IK4306244

Alarm	Attributes	Applicable major release
Name: IK4306244 (8899) Type: equipmentAlarm Package: lte.IK4306244 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 22 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1661 IK4306245

Alarm	Attributes	Applicable major release
Name: IK4306245 (8900) Type: equipmentAlarm Package: lte.IK4306245 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 23 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1662 IK4306246

Alarm	Attributes	Applicable major release
Name: IK4306246 (8901) Type: equipmentAlarm Package: lte.IK4306246 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 24 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1663 IK4306247

Alarm	Attributes	Applicable major release
Name: IK4306247 (8902) Type: equipmentAlarm Package: lte.IK4306247 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 25 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1664 IK4306248

Alarm	Attributes	Applicable major release
Name: IK4306248 (8903) Type: equipmentAlarm Package: lte.IK4306248 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 26 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1665 IK4306249

Alarm	Attributes	Applicable major release
Name: IK4306249 (8904) Type: equipmentAlarm Package: lte.IK4306249 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 27 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1665 IK4306249 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1666 IK4306250

Alarm	Attributes	Applicable major release
Name: IK4306250 (8905) Type: equipmentAlarm Package: lte.IK4306250 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 28 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1667 IK4306251

Alarm	Attributes	Applicable major release
Name: IK4306251 (8906) Type: equipmentAlarm Package: lte.IK4306251 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 29 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1668 IK4306252

Alarm	Attributes	Applicable major release
Name: IK4306252 (8907) Type: equipmentAlarm Package: lte.IK4306252 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 30 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1669 IK4306253

Alarm	Attributes	Applicable major release
Name: IK4306253 (8908) Type: equipmentAlarm Package: lte.IK4306253 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 31 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1670 IK4306254

Alarm	Attributes	Applicable major release
Name: IK4306254 (8909) Type: equipmentAlarm Package: lte.IK4306254 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 32 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1671 IK4306255

Alarm	Attributes	Applicable major release
Name: IK4306255 (8910) Type: processingErrorAlarm Package: lte.IK4306255 Raised on class: lte.Cell	Severity: indeterminate Specific problem: AUTOMATED HANDOVER PARAMETER ADJUSTMENT COMPLETED FOR VOLTE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the SON process that automatically adjusts intra-frequency VoLTE handover parameters has no further adjustments to make.		
Remedial action: None		

Table 29-1672 IK4306256

Alarm	Attributes	Applicable major release
Name: IK4306256 (8911) Type: processingErrorAlarm Package: lte.IK4306256 Raised on class: lte.Cell	Severity: major Specific problem: AUTOMATED HANDOVER PARAMETER ADJUSTMENT NOT POSSIBLE FOR VOLTE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the SON process that automatically adjusts intra-frequency VoLTE handover parameters cannot make any adjustments because of the setting of the configurable limits on the allowed adjustments.		
Remedial action: Modify the VoLTE handover parameter adjustment limits to allow additional values.		

Table 29-1673 IK4306257

Alarm	Attributes	Applicable major release
Name: IK4306257 (8912) Type: qualityOfServiceAlarm Package: lte.IK4306257 Raised on class: lte.Cell	Severity: warning Specific problem: HANDOVER OPTIMIZATION ADJUSTMENT STARTED FOR VOLTE Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates the SON process that adjusts intra-frequency handover parameters has started adjusting handover parameters for VoLTE.		
Remedial action: No action is required. This alarm is provided to allow operator to correlate VoLTE handover optimization adjustment with other issues that may happen in the network at the same time.		

Table 29-1674 IK4306258

Alarm	Attributes	Applicable major release
Name: IK4306258 (8913) Type: processingErrorAlarm Package: lte.IK4306258 Raised on class: lte.Cell	Severity: major Specific problem: SIM HEALTH CHECK PHASE 3 - ASSOCIATED CELL AFFECTED BY RFM LRA Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The OAM System Integrity Monitor has run a Health Check and has found a degraded cell. SIM has raised a critical alarm against the degraded cell and is now initiating Phase 3 recovery actions to initialize the RFMs. This alarm is indicating that this associated cell will be affected by the recovery actions being taken on the RFM.		
Remedial action: No action is required. The alarm should clear after the RFM Recovery Sequence is complete.		

Table 29-1675 IK4306260

Alarm	Attributes	Applicable major release
Name: IK4306260 (8914) Type: equipmentAlarm Package: lte.IK4306260 Raised on class: lte.RFM	Severity: major Specific problem: MULTI-CPRI RFM FIBER LENGTH Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when an excessive difference is detected between the transmission delays of two links from the BBU to a multi-CPRI RRH. The presence of this alarm denotes an excessive difference between the lengths of the two CPRI links reported by the alarm. This alarm should not be present when the two links have the same length.		
Remedial action: The length of the two CPRI links should be equalized.		

Table 29-1676 IK4306261

Alarm	Attributes	Applicable major release
Name: IK4306261 (8915) Type: equipmentAlarm Package: lte.IK4306261 Raised on class: lte.CBCardSpecifics	Severity: major Specific problem: NETCONF QUEUE OVERLOAD Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that all DB update request messages received from eNB are discarded by eNB OAM due \nto Netconf max queue threshold limit 15000 entries. The alarm is cleared when NETCONF QUEUE is back under 10000 entries.		
Remedial action: Reset eNB in next maintenance window.		

Table 29-1677 IK4306262

Alarm	Attributes	Applicable major release
Name: IK4306262 (8916) Type: processingErrorAlarm Package: lte.IK4306262 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: PRIVATE KEYS NOT LOCKED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that RSA private keys are not locked.		
Remedial action: No action is required.		

Table 29-1678 IK4306263

Alarm	Attributes	Applicable major release
Name: IK4306263 (8917) Type: processingErrorAlarm Package: lte.IK4306263 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: RF GAIN SET IS NOTSUPPORTED BY THE HARDWARE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by OAM to set the RF gain of the TmaSubunit failed.		
Remedial action: None.		

Table 29-1679 IK4306264

Alarm	Attributes	Applicable major release
Name: IK4306264 (8918) Type: equipmentAlarm Package: lte.IK4306264 Raised on class: lte.Cell	Severity: critical Specific problem: MULTI CARRIER/SECTOR LICENSE IS NOT SUPPORTED ON HW CONFIGURATION Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the cell configuration for the maximum number of carriers or the maximum number of sectors is not supported by the equipped modem type.		
Remedial action: Verify and correct the configuration data.		

Table 29-1680 IK4306265

Alarm	Attributes	Applicable major release
Name: IK4306265 (8919) Type: equipmentAlarm Package: lte.IK4306265 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: PERIODIC ANTENNA TILT CHECK FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by OAM to update the electrical tilt of the RetSubunit with the value in the database failed after a periodic scan of this data.		
Remedial action: None		

Table 29-1681 IK4306266

Alarm	Attributes	Applicable major release
Name: IK4306266 (8920) Type: operationalViolation Package: lte.IK4306266 Raised on class: lte.RetAldEntry	Severity: minor Specific problem: RET DEVICE NOT FOUND FOR SPECIFIED UNIQUE IDENTIFIER NUMBER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This alarm indicates that there are no RET in the eNodeB with the Unique Identification Number specified in the Work Order.		
Remedial action: The operator should fix the value specified in the Work Order for the RET device.		

Table 29-1682 IK4306267

Alarm	Attributes	Applicable major release
Name: IK4306267 (8921) Type: operationalViolation Package: lte.IK4306267 Raised on class: lte.TmaAldEntry	Severity: minor Specific problem: TMA DEVICE NOT FOUND FOR SPECIFIED UNIQUE IDENTIFIER NUMBER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This alarm indicates that there are no TMA in the eNodeB with the Unique Identification Number specified in the Work Order.		
Remedial action: The operator should fix the value specified in the Work Order for the TMA device.		

Table 29-1683 IK4306268

Alarm	Attributes	Applicable major release
Name: IK4306268 (8922) Type: processingErrorAlarm Package: lte.IK4306268 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: MAXIMUM NUMBER OF ALDS EXCEEDED FOR THE ENODEB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that there are too many TMAs in the eNodeB.		
Remedial action: No action is required.		

Table 29-1684 IK4306269

Alarm	Attributes	Applicable major release
Name: IK4306269 (8923) Type: processingErrorAlarm Package: lte.IK4306269 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: MAXIMUM NUMBER OF ALDS EXCEEDED FOR THE ENODEB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that there are too many RETs in the eNodeB.		
Remedial action: No action is required.		

Table 29-1685 IK4306270

Alarm	Attributes	Applicable major release
Name: IK4306270 (8924) Type: processingErrorAlarm Package: lte.IK4306270 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: TMASUBUNIT IN BYPASS MODE, NO GAIN CHANGE ALLOWED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that an attempt was made to change the gain of a TmaSubunit that was in Bypass Mode.		
Remedial action: .		

Table 29-1686 IK4306271

Alarm	Attributes	Applicable major release
Name: IK4306271 (8925) Type: equipmentAlarm Package: lte.IK4306271 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP SERVER FUNCTION ACTIVATION/DEACTIVATION FAILURE CHECK FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The event indicates that the TWAMP server activation/de-activation fails on the eNB.		
Remedial action: None		

Table 29-1687 IK4306272

Alarm	Attributes	Applicable major release
Name: IK4306272 (8926) Type: equipmentAlarm Package: lte.IK4306272 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP SERVER CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The event indicates that the TWAMP server configuration on a given Vlan fails.		
Remedial action: None		

Table 29-1688 IK4306273

Alarm	Attributes	Applicable major release
Name: IK4306273 (8927) Type: equipmentAlarm Package: lte.IK4306273 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TWAMP SERVER CONFIGURATION SUCCESS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that configuration of the TWAMP server on an IP address and port was successful.		
Remedial action: No action is required.		

Table 29-1689 IK4306274

Alarm	Attributes	Applicable major release
Name: IK4306274 (8928) Type: processingErrorAlarm Package: lte.IK4306274 Raised on class: lte.Cell	Severity: warning Specific problem: ANTENNA_PORT RX DEACTIVATED Implicitly cleared: true Default probable cause: configurationOrCustomizationError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when inconsistent configuration data between CellAntennaPort::rxPath =" TRUE and AntennaPort::rxUsed =FALSE is imported directly from xml file. (If LteCell.CellAntennaPath.rxPath is True, then the value of rxUsed in the associated AntennaPort instance must be True. This rule is enforced by WPS if the change is through NEM. But when the change is through importing xml file, there is no such enforcement and alarm."		
Remedial action: Need operator to correct the inconsistent configuration data		

Table 29-1690 IK4306275

Alarm	Attributes	Applicable major release
Name: IK4306275 (8929) Type: processingErrorAlarm Package: lte.IK4306275 Raised on class: lte.Cell	Severity: warning Specific problem: ANTENNA_PORT TX DEACTIVATED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when inconsistent configuration data between CellAntennaPort::txPath =" TRUE and AntennaPort::txUsed =FALSE is imported directly from xml file. (If LteCell.CellAntennaPath.txPath is True, then the value of txUsed in the associated AntennaPort instance must be True. This rule is enforced by WPS if the change is through NEM. But when the change is through importing xml file, there is no such enforcement and alarm."		
Remedial action: Need operator to correct the inconsistent configuration data		

Table 29-1691 IK4306278

Alarm	Attributes	Applicable major release
Name: IK4306278 (10135) Type: processingErrorAlarm Package: lte.IK4306278 Raised on class: lte.AntennaPort	Severity: major Specific problem: OAM ANTENNA_PORT ALARM 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified OAM antenna port fault		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1692 IK4306279

Alarm	Attributes	Applicable major release
Name: IK4306279 (10136) Type: equipmentAlarm Package: lte.IK4306279 Raised on class: lte.EthernetPort	Severity: warning Specific problem: OAM ETHERNET PORT FAULT 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1693 IK4306280

Alarm	Attributes	Applicable major release
Name: IK4306280 (10137) Type: qualityOfServiceAlarm Package: lte.IK4306280 Raised on class: lte.EthernetPort	Severity: major Specific problem: OAM ETHERNET PORT FAULT 2 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1694 IK4306281

Alarm	Attributes	Applicable major release
Name: IK4306281 (10138) Type: qualityOfServiceAlarm Package: lte.IK4306281 Raised on class: lte.EthernetPort	Severity: minor Specific problem: OAM ETHERNET PORT FAULT 3 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1695 IK4306282

Alarm	Attributes	Applicable major release
Name: IK4306282 (10139) Type: equipmentAlarm Package: lte.IK4306282 Raised on class: lte.M3MmeTransportLayerAccess	Severity: major Specific problem: M3 TRANS FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-1696 IK4306283

Alarm	Attributes	Applicable major release
Name: IK4306283 (10140) Type: equipmentAlarm Package: lte.IK4306283 Raised on class: lte.M3MmeTransportLayerAccess	Severity: major Specific problem: M3 TRANS FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS fault detected.		

Table 29-1696 IK4306283 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Not Relevant for a Spare Alarm		

Table 29-1697 IK4306284

Alarm	Attributes	Applicable major release
Name: IK4306284 (10141) Type: equipmentAlarm Package: lte.IK4306284 Raised on class: lte.M3MmeTransportLayerAccess	Severity: minor Specific problem: M3 TRANS FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified M3 TRANS fault detected.		
Remedial action: Not Relevant for a Spare Alarm		

Table 29-1698 IK4306285

Alarm	Attributes	Applicable major release
Name: IK4306285 (10142) Type: equipmentAlarm Package: lte.IK4306285 Raised on class: lte.RFM	Severity: minor Specific problem: OAM RFM FAULT 1 Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1699 IK4306286

Alarm	Attributes	Applicable major release
Name: IK4306286 (10143) Type: processingErrorAlarm Package: lte.IK4306286 Raised on class: lte.RFM	Severity: major Specific problem: OAM RFM FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1700 IK4306287

Alarm	Attributes	Applicable major release
Name: IK4306287 (10144) Type: equipmentAlarm Package: lte.IK4306287 Raised on class: lte.RFM	Severity: major Specific problem: OAM RFM FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1701 IK4306288

Alarm	Attributes	Applicable major release
Name: IK4306288 (10145) Type: processingErrorAlarm Package: lte.IK4306288 Raised on class: lte.RFM	Severity: critical Specific problem: OAM RFM FAULT 4 Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Call the next level of support.		

Table 29-1702 IK4306289

Alarm	Attributes	Applicable major release
Name: IK4306289 (10146) Type: equipmentAlarm Package: lte.IK4306289 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-1703 IK4306290

Alarm	Attributes	Applicable major release
Name: IK4306290 (10147) Type: processingErrorAlarm Package: lte.IK4306290 Raised on class: lte.RFM	Severity: indeterminate Specific problem: OAM RFM EVENT 2 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare event for future use.		
Remedial action: None.		

Table 29-1704 IK4306292

Alarm	Attributes	Applicable major release
Name: IK4306292 (10148) Type: processingErrorAlarm Package: lte.IK4306292 Raised on class: lte.RFM	Severity: indeterminate Specific problem: AISG COMMAND FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt to send a command by the operator to a ALD unit failed.		
Remedial action: No action is required.		

Table 29-1705 IK4306294

Alarm	Attributes	Applicable major release
Name: IK4306294 (10149) Type: operationalViolation Package: lte.IK4306294 Raised on class: lte.RFM	Severity: indeterminate Specific problem: NO RAE OBJECT FOUND UNDER THE RRH Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the operator miss-configured the CpriRadioEquipment by setting the parameter isRaeEnabled to True for a RRH that does not have a RAE unit.		
Remedial action: Set the parameter to False or verify that a RAE unit is properly connected to the RRH.		

Table 29-1706 IK4306295

Alarm	Attributes	Applicable major release
Name: IK4306295 (10150) Type: equipmentAlarm Package: lte.IK4306295 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: MAXIMUM NUMBER OF ALDS EXCEEDED FOR THE ENODEB Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that there are too many ALD types RET or TMA or RAE attached to the eNodeB		
Remedial action: The extra ALD unit must be removed from the eNodeB.		

Table 29-1707 IK4306296

Alarm	Attributes	Applicable major release
Name: IK4306296 (10151) Type: equipmentAlarm Package: lte.IK4306296 Raised on class: lte.RFM	Severity: indeterminate Specific problem: AISG HOST IS LOCKED OR DISABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L

Table 29-1707 IK4306296 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the eNodeB OAM was not able to send a message to the ALD device because the RFM that controls the AISG bus where the ALD resides is locked or disabled.		
Remedial action: Reset the RFM that controls the AISG bus where the ALD resides.		

Table 29-1708 IK4306297

Alarm	Attributes	Applicable major release
Name: IK4306297 (10152) Type: processingErrorAlarm Package: lte.IK4306297 Raised on class: lte.Cell	Severity: critical Specific problem: CELL CRITICAL CONFIGURATION ERROR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates there is a critical error in the configuration of the cell.		
Remedial action: Operator must set the attribute(s) in error to a value consistent with the configuration of the LteCell.		

Table 29-1709 IK4306298

Alarm	Attributes	Applicable major release
Name: IK4306298 (10153) Type: processingErrorAlarm Package: lte.IK4306298 Raised on class: lte.ENBEquipment	Severity: warning Specific problem: CONFIGURED ENB MODE NOT SUPPORTED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the configured enb mode can't be supported by eNB		
Remedial action: Operator must set Enb::modeConf to a value which can be supported by eNB.		

Table 29-1710 IK4306299

Alarm	Attributes	Applicable major release
Name: IK4306299 (10154) Type: processingErrorAlarm Package: lte.IK4306299 Raised on class: lte.Cell	Severity: major Specific problem: SIM HEALTH CHECK PHASE 1 - RX RSSI DEGRADED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNB, has detected a degraded RX RSSI on the cell. This is the SIM Phase 1 detection.		

Table 29-1710 IK4306299 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required. If the degradation persists, SIM may escalate to Local Recovery Action on the implicated cell.		

Table 29-1711 IK4306300

Alarm	Attributes	Applicable major release
Name: IK4306300 (10155) Type: processingErrorAlarm Package: lte.IK4306300 Raised on class: lte.Cell	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 2 - RX RSSI DEGRADED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNB, has detected a degraded RX RSSI that has persisted beyond the configurable limit. This is the SIM Phase 2 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1712 IK4306301

Alarm	Attributes	Applicable major release
Name: IK4306301 (10156) Type: processingErrorAlarm Package: lte.IK4306301 Raised on class: lte.RFM	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - RX RSSI DEGRADED Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNB cell, has detected an active antenna receive path with degraded RSSI continually for the Phase 3 detection period.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1713 IK4306305

Alarm	Attributes	Applicable major release
Name: IK4306305 (10157) Type: processingErrorAlarm Package: lte.IK4306305 Raised on classes: • lte.RFM • lte.CBCardSpecifics	Severity: major Specific problem: MODULE CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure to configure the module.		

Table 29-1713 IK4306305 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Reset the module. If the alarm persists, reset the full eNodeB. If the alarm still persists, replace the module.		

Table 29-1714 IK4306306

Alarm	Attributes	Applicable major release
Name: IK4306306 (10158) Type: equipmentAlarm Package: lte.IK4306306 Raised on class: lte.Rae	Severity: minor Specific problem: WEIGHTING FACTORS ARE MISSING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB was not able to retrieve Weighting Factors values from the RAE unit.		
Remedial action: Download the Weighting Factors File to the RAE unit.		

Table 29-1715 IK4306307

Alarm	Attributes	Applicable major release
Name: IK4306307 (10159) Type: equipmentAlarm Package: lte.IK4306307 Raised on class: lte.Rae	Severity: minor Specific problem: NO WEIGHTING FACTORS ARE MISSING Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB was not able to retrieve Weighting Factors values from the RAE unit.		
Remedial action: Download the Weighting Factors File to the RAE unit.		

Table 29-1716 IK4306308

Alarm	Attributes	Applicable major release
Name: IK4306308 (10160) Type: securityServiceOrMechanismViolation Package: lte.IK4306308 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB PASSWORD SOON TO EXPIRE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that an eNB account password is about to expire. The eNB account name and the number of days until the password expires are available in the Additional Information field of the event.		
Remedial action: Operator must change the password of the eNB account before it expires.		

Table 29-1717 IK4306309

Alarm	Attributes	Applicable major release
Name: IK4306309 (10161) Type: securityServiceOrMechanismViolation Package: lte.IK4306309 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ENB PASSWORD HAS EXPIRED Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that an eNB account password has expired. The eNB account name is available in the Additional Information field of the event.		
Remedial action: Operator must change the password of the eNB account as soon as possible.		

Table 29-1718 IK4306310

Alarm	Attributes	Applicable major release
Name: IK4306310 (10162) Type: processingErrorAlarm Package: lte.IK4306310 Raised on class: lte.IPsecTunnelConf	Severity: major Specific problem: IPSEC TUNNEL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates the failure of the IPsec tunnel.		
Remedial action: Check the IP Security configuration.		

Table 29-1719 IK4306311

Alarm	Attributes	Applicable major release
Name: IK4306311 (10163) Type: processingErrorAlarm Package: lte.IK4306311 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - CELL OUTAGE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the zero RRC attempt rate has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1720 IK4306315

Alarm	Attributes	Applicable major release
Name: IK4306315 (10164) Type: processingErrorAlarm Package: lte.IK4306315 Raised on classes: • lte.RFM • lte.RFME	Severity: critical Specific problem: SIM HEALTH CHECK PHASE 3 - LOW RRC SUCCESS RATE Implicitly cleared: true Default probable cause: softwareProgramError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the System Integrity Monitor, monitoring the health of the eNodeB, has detected that the RRC Success Rate degradation has persisted beyond the configurable limit. This is the SIM Phase 3 detection.		
Remedial action: No action is required. If SIM escalation to Local Recovery Action is allowed, SIM will automatically trigger Local Recovery Action to try to restore service on this cell.		

Table 29-1721 IK4306317

Alarm	Attributes	Applicable major release
Name: IK4306317 (10165) Type: equipmentAlarm Package: lte.IK4306317 Raised on classes: • lte.M3MmeTransportLayerAccess • lte.X2TransportLayerAccess • lte.MmeTransportLayerAccess	Severity: major Specific problem: TRANS ASSOCIATION DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a S1/M3/X2 association fault respectively between eNodeB and MME, 2 neighboring eNodeB.		
Remedial action: 1. Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME, or between neighboring eNB.		

Table 29-1722 IK4306320

Alarm	Attributes	Applicable major release
Name: IK4306320 (10166) Type: equipmentAlarm Package: lte.IK4306320 Raised on classes: • lte.M3MmeTransportLayerAccess • lte.MmeTransportLayerAccess	Severity: major Specific problem: TRANS ASSOCIATION FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the MME/eNeighboring eNB does not acknowledge the S1/M3//X2 association request from the eNodeB.		
Remedial action: 1.Check IP and SCTP provisioning in eNB and MME. 2. Check network connectivity between eNB and MME, or beween eNB.		

Table 29-1723 IK4306323

Alarm	Attributes	Applicable major release
Name: IK4306323 (10167) Type: processingErrorAlarm Package: lte.IK4306323 Raised on classes: • lte.X2TransportLayerAccess • lte.MmeTransportLayerAccess	Severity: major Specific problem: IP ADDRESS CONFIGURATION DATA MISMATCH Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the IP address is not well filled for the ipFormat specified in Vlan		
Remedial action: Verify and correct the configuration data.		

Table 29-1724 IK4306325

Alarm	Attributes	Applicable major release
Name: IK4306325 (10168) Type: processingErrorAlarm Package: lte.IK4306325 Raised on class: lte.Rae	Severity: indeterminate Specific problem: WEIGHTING FACTOR FILE DOWNLOAD COMPLETED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the download of a Weighting Factor File to the RAESUBUNIT completed.		
Remedial action: None		

Table 29-1725 IK4306326

Alarm	Attributes	Applicable major release
Name: IK4306326 (10169) Type: processingErrorAlarm Package: lte.IK4306326 Raised on class: lte.Rae	Severity: indeterminate Specific problem: WEIGHTING FACTOR FILE DOWNLOAD IN PROGRESS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the download of a Weighting Factor File to the RAESUBUNIT is in progress.		
Remedial action: None		

Table 29-1726 IK4306327

Alarm	Attributes	Applicable major release
Name: IK4306327 (10170) Type: processingErrorAlarm Package: lte.IK4306327 Raised on classes: • lte.RFM • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: indeterminate Specific problem: AISG COMMAND FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt to send a command by the operator to a RET/TMA/RAE unit /RRH/TRDU failed.		
Remedial action: No action is required.		

Table 29-1727 IK4306329

Alarm	Attributes	Applicable major release
Name: IK4306329 (10171) Type: processingErrorAlarm Package: lte.IK4306329 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry	Severity: indeterminate Specific problem: SET DEVICE DATA COMMAND FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by the operator to write to one of the additional data record failed.		
Remedial action: No action is required.		

Table 29-1728 IK4306331

Alarm	Attributes	Applicable major release
Name: IK4306331 (10172) Type: processingErrorAlarm Package: lte.IK4306331 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry • lte.Rae	Severity: indeterminate Specific problem: GET DEVICE DATA COMMAND FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt by OAM to read one of the additional data record failed.		
Remedial action: None.		

Table 29-1729 IK4306334

Alarm	Attributes	Applicable major release
Name: IK4306334 (10173) Type: processingErrorAlarm Package: lte.IK4306334 Raised on classes: • lte.RetAldEntry • lte.TmaAldEntry	Severity: indeterminate Specific problem: UNREACHABLE TARGET OBJECT Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the attempt to send a command by the operator to a TMA/RET failed.		
Remedial action: No action is required.		

Table 29-1730 IK4306336

Alarm	Attributes	Applicable major release
Name: IK4306336 (10174) Type: processingErrorAlarm Package: lte.IK4306336 Raised on classes: • lte.RFM • lte.RFME	Severity: indeterminate Specific problem: SIM LOCAL RECOVERY ACTION Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: The OAM System Integrity Monitor has run a Health Check on the cell and has detected a degradation affecting cell performance. SIM has raised a critical alarm and is now initiating Phase 3 recovery actions to initialize the RFM.		
Remedial action: No action is required.		

Table 29-1731 IK4306338

Alarm	Attributes	Applicable major release
Name: IK4306338 (10175) Type: equipmentAlarm Package: lte.IK4306338 Raised on classes: • lte.RFME • lte.TRDU • lte.ENBEquipment • lte.RRH	Severity: minor Specific problem: HW TYPE NOT ALLOWED BY ENB TYPE LICENSE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the licence for the eNB type does not allow this HW type (RFME/RRH/TRDU/Modem). The performance of this HW type goes beyond what the licence for the eNB type allows		
Remedial action: No action is required. The operator has to use another and appropriate RFME/RRH/TRDU/Modem.		

Table 29-1732 IK4306348

Alarm	Attributes	Applicable major release
Name: IK4306348 (10176) Type: processingErrorAlarm Package: lte.IK4306348 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TROUBLESHOOTING TOOL START Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: A troubleshooting tool has been started. The additional info provides information about the troubleshooting tool invocation.		
Remedial action: No action is required.		

Table 29-1733 IK4306349

Alarm	Attributes	Applicable major release
Name: IK4306349 (10177) Type: processingErrorAlarm Package: lte.IK4306349 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: TROUBLESHOOTING TOOL STOP Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: A troubleshooting tool has been stopped. The additional info provides information about the troubleshooting tool and reasons for termination.		
Remedial action: No action is required.		

Table 29-1734 IK4306351

Alarm	Attributes	Applicable major release
Name: IK4306351 (10178) Type: equipmentAlarm Package: lte.IK4306351 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: OTDOA NOT SUPPORTABLE Implicitly cleared: true Default probable cause: degradedSignal	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that OTDOA service is suspended because the GPS signal is too unstable to support OTDOA service.		
Remedial action: Disable OTDOA or check for proper GPS antenna placement. System reset required.		

Table 29-1735 IK4306352

Alarm	Attributes	Applicable major release
Name: IK4306352 (10179) Type: processingErrorAlarm Package: lte.IK4306352 Raised on class: lte.PerOperatorTransportConf	Severity: major Specific problem: CMS INIT FAILED (ERROR) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L

Table 29-1735 IK4306352 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates CMS(Certificate Management Support) initialization request failure due to an error.		
Remedial action: Check the Sub CMS configuration. Verify and correct the CMS configuration data based on the error code received. Check the network connection. eNB has to get the valid operator-signed certificate(s) before the concerned traffic can be resumed.		

Table 29-1736 IK4306353

Alarm	Attributes	Applicable major release
Name: IK4306353 (10180) Type: processingErrorAlarm Package: lte.IK4306353 Raised on class: lte.PerOperatorTransportConf	Severity: major Specific problem: CMS INIT FAILED (TIMEOUT) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates CMS(Certificate Management Support) initialization request failure due to timeout.		
Remedial action: eNB has to get the valid operator-signed certificate(s) before the concerned traffic can be resumed.\nCheck the network connection, then check IP connectivity, HTTP connectivity and Sub CMS/CMS server connectivity.\nCheck the Sub CMS/CMS configuration.		

Table 29-1737 IK4306354

Alarm	Attributes	Applicable major release
Name: IK4306354 (10181) Type: processingErrorAlarm Package: lte.IK4306354 Raised on class: lte.PerOperatorTransportConf	Severity: major Specific problem: CMS KEY UPDATE FAILED (ERROR) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates CMS(Certificate Management Support) key update failure due to an error.		
Remedial action: Check the Sub CMS configuration. Verify and correct the CMS configuration data based on the error code received.		

Table 29-1738 IK4306355

Alarm	Attributes	Applicable major release
Name: IK4306355 (10182) Type: processingErrorAlarm Package: lte.IK4306355 Raised on class: lte.PerOperatorTransportConf	Severity: major Specific problem: CMS KEY UPDATE FAILED (TIMEOUT) Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates CMS(Certificate Management Support) key update activity failure due to timeout.		

Table 29-1738 IK4306355 (continued)

Alarm	Attributes	Applicable major release
Remedial action: The eNodeB did not receive a message response back from the Sub-CMS during a CMP message exchange.\nThe timeout could be because the Sub CMS is not online or the CMS IP address was incorrect or the network is down or some other failure reason.		

Table 29-1739 IK4306356

Alarm	Attributes	Applicable major release
Name: IK4306356 (10183) Type: processingErrorAlarm Package: lte.IK4306356 Raised on class: lte.PerOperatorTransportConf	Severity: major Specific problem: OPERATOR CERTIFICATE ENROLLMENT ERROR Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that certificate enrollment can not be started because no authentication credentials were found.		
Remedial action: Provide the shared key for authentication of CMPv2 messages . eNodeB uses a shared key for authentication to Sub CMS when performing certificate enrollment.		

Table 29-1740 IK4306357

Alarm	Attributes	Applicable major release
Name: IK4306357 (10184) Type: equipmentAlarm Package: lte.IK4306357 Raised on class: lte.CBCardSpecifics	Severity: critical Specific problem: LOSS OF TDD PHASE SYNC Implicitly cleared: true Default probable cause: lossOfSignal	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the phase-sync requirement for supporting TDD can no longer be guaranteed due to the loss of clock reference.		
Remedial action: If alarm remains consider the Clock reference alarms to determine the cause of the onset of holdover.		

Table 29-1741 IK4306358

Alarm	Attributes	Applicable major release
Name: IK4306358 (10185) Type: equipmentAlarm Package: lte.IK4306358 Raised on class: lte.RFM	Severity: critical Specific problem: ALL ANTENNA_PORT FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that all configured antenna ports of the RFM have failed.		
Remedial action: Check other alarms raised for this RFM to determine whether a configuration problem or a hardware failure exists. Reset the RFM, if unsuccessful, replace the unit.		

Table 29-1742 IK4306359

Alarm	Attributes	Applicable major release
Name: IK4306359 (10186) Type: equipmentAlarm Package: lte.IK4306359 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1743 IK4306360

Alarm	Attributes	Applicable major release
Name: IK4306360 (10187) Type: equipmentAlarm Package: lte.IK4306360 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1744 IK4306361

Alarm	Attributes	Applicable major release
Name: IK4306361 (10188) Type: equipmentAlarm Package: lte.IK4306361 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1745 IK4306362

Alarm	Attributes	Applicable major release
Name: IK4306362 (10189) Type: equipmentAlarm Package: lte.IK4306362 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1745 IK4306362 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1746 IK4306363

Alarm	Attributes	Applicable major release
Name: IK4306363 (10190) Type: equipmentAlarm Package: lte.IK4306363 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1747 IK4306364

Alarm	Attributes	Applicable major release
Name: IK4306364 (10191) Type: equipmentAlarm Package: lte.IK4306364 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1748 IK4306365

Alarm	Attributes	Applicable major release
Name: IK4306365 (10192) Type: equipmentAlarm Package: lte.IK4306365 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1749 IK4306366

Alarm	Attributes	Applicable major release
Name: IK4306366 (10193) Type: equipmentAlarm Package: lte.IK4306366 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1750 IK4306367

Alarm	Attributes	Applicable major release
Name: IK4306367 (10194) Type: equipmentAlarm Package: lte.IK4306367 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 9 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1751 IK4306368

Alarm	Attributes	Applicable major release
Name: IK4306368 (10195) Type: equipmentAlarm Package: lte.IK4306368 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 12 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1752 IK4306369

Alarm	Attributes	Applicable major release
Name: IK4306369 (10196) Type: equipmentAlarm Package: lte.IK4306369 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 10 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1752 IK4306369 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1753 IK4306370

Alarm	Attributes	Applicable major release
Name: IK4306370 (10197) Type: equipmentAlarm Package: lte.IK4306370 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 11 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1754 IK4306371

Alarm	Attributes	Applicable major release
Name: IK4306371 (10198) Type: equipmentAlarm Package: lte.IK4306371 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 13 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1755 IK4306372

Alarm	Attributes	Applicable major release
Name: IK4306372 (10199) Type: equipmentAlarm Package: lte.IK4306372 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 14 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1756 IK4306373

Alarm	Attributes	Applicable major release
Name: IK4306373 (10200) Type: equipmentAlarm Package: lte.IK4306373 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 16 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1757 IK4306374

Alarm	Attributes	Applicable major release
Name: IK4306374 (10201) Type: equipmentAlarm Package: lte.IK4306374 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 15 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1758 IK4306375

Alarm	Attributes	Applicable major release
Name: IK4306375 (10202) Type: equipmentAlarm Package: lte.IK4306375 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 17 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1759 IK4306376

Alarm	Attributes	Applicable major release
Name: IK4306376 (10203) Type: equipmentAlarm Package: lte.IK4306376 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 18 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1759 IK4306376 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1760 IK4306377

Alarm	Attributes	Applicable major release
Name: IK4306377 (10204) Type: equipmentAlarm Package: lte.IK4306377 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 20 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1761 IK4306378

Alarm	Attributes	Applicable major release
Name: IK4306378 (10205) Type: equipmentAlarm Package: lte.IK4306378 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 19 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1762 IK4306379

Alarm	Attributes	Applicable major release
Name: IK4306379 (10206) Type: equipmentAlarm Package: lte.IK4306379 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 21 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1763 IK4306380

Alarm	Attributes	Applicable major release
Name: IK4306380 (10207) Type: equipmentAlarm Package: lte.IK4306380 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 22 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1764 IK4306381

Alarm	Attributes	Applicable major release
Name: IK4306381 (10208) Type: equipmentAlarm Package: lte.IK4306381 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 23 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1765 IK4306382

Alarm	Attributes	Applicable major release
Name: IK4306382 (10209) Type: equipmentAlarm Package: lte.IK4306382 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 24 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1766 IK4306383

Alarm	Attributes	Applicable major release
Name: IK4306383 (10210) Type: equipmentAlarm Package: lte.IK4306383 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 25 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1766 IK4306383 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1767 IK4306384

Alarm	Attributes	Applicable major release
Name: IK4306384 (10211) Type: equipmentAlarm Package: lte.IK4306384 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 26 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1768 IK4306385

Alarm	Attributes	Applicable major release
Name: IK4306385 (10212) Type: equipmentAlarm Package: lte.IK4306385 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 27 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1769 IK4306386

Alarm	Attributes	Applicable major release
Name: IK4306386 (10213) Type: equipmentAlarm Package: lte.IK4306386 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 28 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1770 IK4306387

Alarm	Attributes	Applicable major release
Name: IK4306387 (10214) Type: equipmentAlarm Package: lte.IK4306387 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 29 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1771 IK4306388

Alarm	Attributes	Applicable major release
Name: IK4306388 (10215) Type: equipmentAlarm Package: lte.IK4306388 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 30 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1772 IK4306389

Alarm	Attributes	Applicable major release
Name: IK4306389 (10216) Type: equipmentAlarm Package: lte.IK4306389 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 31 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1773 IK4306390

Alarm	Attributes	Applicable major release
Name: IK4306390 (10217) Type: equipmentAlarm Package: lte.IK4306390 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: DBU EXTERNAL CONTACT CHANGE 32 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1773 IK4306390 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates a change in the external user alarm contact state.		
Remedial action: Check the user equipment.		

Table 29-1774 IK4306391

Alarm	Attributes	Applicable major release
Name: IK4306391 (10218) Type: equipmentAlarm Package: lte.IK4306391 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1775 IK4306392

Alarm	Attributes	Applicable major release
Name: IK4306392 (10219) Type: equipmentAlarm Package: lte.IK4306392 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1776 IK4306393

Alarm	Attributes	Applicable major release
Name: IK4306393 (10220) Type: equipmentAlarm Package: lte.IK4306393 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1777 IK4306394

Alarm	Attributes	Applicable major release
Name: IK4306394 (10221) Type: equipmentAlarm Package: lte.IK4306394 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1778 IK4306395

Alarm	Attributes	Applicable major release
Name: IK4306395 (10222) Type: equipmentAlarm Package: lte.IK4306395 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1779 IK4306396

Alarm	Attributes	Applicable major release
Name: IK4306396 (10223) Type: equipmentAlarm Package: lte.IK4306396 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1780 IK4306397

Alarm	Attributes	Applicable major release
Name: IK4306397 (10224) Type: equipmentAlarm Package: lte.IK4306397 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1780 IK4306397 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1781 IK4306398

Alarm	Attributes	Applicable major release
Name: IK4306398 (10225) Type: equipmentAlarm Package: lte.IK4306398 Raised on class: lte.RFM	Severity: indeterminate Specific problem: RFM EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the external alarm wired to the RFM has changed state.		
Remedial action: Check the attached user equipment.		

Table 29-1782 IK4306399

Alarm	Attributes	Applicable major release
Name: IK4306399 (10226) Type: equipmentAlarm Package: lte.IK4306399 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1783 IK4306400

Alarm	Attributes	Applicable major release
Name: IK4306400 (10227) Type: equipmentAlarm Package: lte.IK4306400 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1784 IK4306401

Alarm	Attributes	Applicable major release
Name: IK4306401 (10228) Type: equipmentAlarm Package: lte.IK4306401 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1785 IK4306402

Alarm	Attributes	Applicable major release
Name: IK4306402 (10229) Type: equipmentAlarm Package: lte.IK4306402 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 4 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1786 IK4306403

Alarm	Attributes	Applicable major release
Name: IK4306403 (10230) Type: equipmentAlarm Package: lte.IK4306403 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 5 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1787 IK4306404

Alarm	Attributes	Applicable major release
Name: IK4306404 (10231) Type: equipmentAlarm Package: lte.IK4306404 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 6 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1787 IK4306404 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1788 IK4306405

Alarm	Attributes	Applicable major release
Name: IK4306405 (10232) Type: equipmentAlarm Package: lte.IK4306405 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 7 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1789 IK4306406

Alarm	Attributes	Applicable major release
Name: IK4306406 (10233) Type: equipmentAlarm Package: lte.IK4306406 Raised on class: lte.AMR	Severity: indeterminate Specific problem: AMR EXTERNAL CONTACT CHANGE 8 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the RF cabinet external contact for the user alarm closure has changed.		
Remedial action: Check the user equipment.		

Table 29-1790 IK4306410

Alarm	Attributes	Applicable major release
Name: IK4306410 (10234) Type: qualityOfServiceAlarm Package: lte.IK4306410 Raised on class: lte.Cell	Severity: indeterminate Specific problem: WEIGHTING FACTORS VALUES NO LONGER VALID Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the Beamforming values that are used by the LteCell are not longer valid because the new electrical tilt value is not related to the electrical tilt value that used to retrieve the WF values that are in used by the LteCell.		
Remedial action: None. The operator will need to reconfigure the LteCell by specifying the electrical tilt value to be used to select a new set of Weighting Factors values.		

Table 29-1791 IK4306411

Alarm	Attributes	Applicable major release
Name: IK4306411 (10235) Type: qualityOfServiceAlarm Package: lte.IK4306411 Raised on class: lte.Cell	Severity: warning Specific problem: RAE UNIT NOT AVAILABLE FOR WEIGHTING FACTORS Implicitly cleared: true Default probable cause: performanceDegraded	Release: • LR16.1.L • LR16.2.L
Description: This warning alarm indicates that the Weighting Factors values could not be retrieved from the RAE unit because it was locked or disabled. The LteCell was configured using other parameters. The alarm shall remain set until the LteCell can be reconfigured using the values from the Rae unit.		
Remedial action: None. The operator will need to unlock the RAE or execute a reset action to see if the loss of communication alarm clears. Once the RAE unit is Unlock and the loss of communication alarm has cleared, the LteCell must be reset so that the WF values are retrieved from the RAE unit.		

Table 29-1792 IK4306412

Alarm	Attributes	Applicable major release
Name: IK4306412 (11032) Type: integrityViolation Package: lte.IK4306412 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CM INTEGRITY CHECK REPORT Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that an integrity check has run in the eNB and is reporting the results.		
Remedial action: No action is required.		

Table 29-1793 IK4306413

Alarm	Attributes	Applicable major release
Name: IK4306413 (11033) Type: equipmentAlarm Package: lte.IK4306413 Raised on class: lte.Cell	Severity: critical Specific problem: ENODEB SOFTWARE DOES NOT SUPPORT THE REQUESTED CELL CONFIGURATION Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the configuration assigned to the cell is not supported by the installed software.		
Remedial action: Revert to previous running configuration/software. Contact the support team to check the software content.		

Table 29-1794 IK4306414

Alarm	Attributes	Applicable major release
Name: IK4306414 (11034) Type: equipmentAlarm Package: lte.IK4306414 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: PTP PDV PROFILE UNAVAILABLE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the PDV profile file requested is not present in the eNB.		
Remedial action: As the profile requested is not available, the synchronization timing algorithm is using the predefined profile1(0). If this default profile is not acceptable, please, load a new custom profile file and restart the eNB		

Table 29-1795 IK4306416

Alarm	Attributes	Applicable major release
Name: IK4306416 (11035) Type: equipmentAlarm Package: lte.IK4306416 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: PTP PDV PROFILE HAS ERRORS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the PDV profile file requested can not be used in the eNB due to errors in it.		
Remedial action: The synchronization timing algorithm is using the (default) predefined profile1(0). You must load a new profile with no error in it and restart the eNB.		

Table 29-1796 IK4306418

Alarm	Attributes	Applicable major release
Name: IK4306418 (11036) Type: processingErrorAlarm Package: lte.IK4306418 Raised on class: lte.Cell	Severity: critical Specific problem: CELL CANNOT BE ASSIGNED TO MODEM Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates this cell can't be mapped to modem.		
Remedial action: Operator may need to change the MIM configuration according to the guide of alarm additional information.		

Table 29-1797 IK4306419

Alarm	Attributes	Applicable major release
Name: IK4306419 (11037) Type: processingErrorAlarm Package: lte.IK4306419 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: PASSWORD PARAM CONFIGURATION FAILURE Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR16.1.L • LR16.2.L
Description: This alarm is raised if a configuration change to a password validity parameter fails after the successful Netconf reply has been returned to the EMS.		
Remedial action: When the eNB is not busy with other password commands, execute the Reverse Work Order for the password validity parameter change and then re-execute the original Work Order. Or reset the eNB to trigger a synchronization of the eNB password files with the eNB database.		

Table 29-1798 IK4306420

Alarm	Attributes	Applicable major release
Name: IK4306420 (11038) Type: equipmentAlarm Package: lte.IK4306420 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: VNF VM USAGE OUT OF BOUNDS Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that vBBU VNF VMs CPU usage is high or low for scalability.		
Remedial action: The vBBU horizontal scaling operation need to be executed according to the content of the additional information of the alarm.		

Table 29-1799 IK4306421

Alarm	Attributes	Applicable major release
Name: IK4306421 (11039) Type: equipmentAlarm Package: lte.IK4306421 Raised on class: lte.RRH	Severity: minor Specific problem: RAE BEAMFORMING NOT SUPPORTED BY SW Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This spare alarm indicates that Beamforming using data from RAE unit was enabled on the CpriRadioEquipment and this is not supported by OAM and CallP.		
Remedial action: Configuration is accepted but the eNodeB OAM will use the Beamforming configuration parameters instead of data from the Rae Unit. The alarm shall remain set until a new configuration update is received with the parameter set to False.		

Table 29-1800 IK4306422

Alarm	Attributes	Applicable major release
Name: IK4306422 (11040) Type: equipmentAlarm Package: lte.IK4306422 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MODEM RESET REQUIRED FOR RECONFIGURATION Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that online cell(s) creation operation is ongoing involving modem resource reset(s). Potential impacts on existing cells (cell outage) can occur.		
Remedial action: No action is required.		

Table 29-1801 IK4306423

Alarm	Attributes	Applicable major release
Name: IK4306423 (11041) Type: processingErrorAlarm Package: lte.IK4306423 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: INTER-BBU SWITCH FIRMWARE OR CONFIGURATION FILE UPGRADE FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only.\nIt indicates a failure during either the upgrade of the firmware or the upgrade of the configuration file of the Inter-BBU Switch (a.k.a SRIO Switch Box).		
Remedial action: Check the firmware and the configuration file of the Inter-BBU Switch (a.k.a. SRIO Switch Box) are correct. Once correct, please retry the eNB Software Upgrade procedure of the eNB.		

Table 29-1802 IK4306424

Alarm	Attributes	Applicable major release
Name: IK4306424 (11042) Type: equipmentAlarm Package: lte.IK4306424 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: major Specific problem: OSC OVER TEMP Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the controller's timing oscillator temperature is above the specification limit.		
Remedial action: Check for proper fan operation and that fan is compatible with hardware configuration, check system inlet temperature is within operating range. Check for shelf fan, cabinet fan and air filter alarms. Replace the controller unit if necessary.		

Table 29-1803 IK4306425

Alarm	Attributes	Applicable major release
Name: IK4306425 (11043) Type: equipmentAlarm Package: lte.IK4306425 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: SRIOSW FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1804 IK4306426

Alarm	Attributes	Applicable major release
Name: IK4306426 (11044) Type: equipmentAlarm Package: lte.IK4306426 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: SRIOSW FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1805 IK4306427

Alarm	Attributes	Applicable major release
Name: IK4306427 (11045) Type: equipmentAlarm Package: lte.IK4306427 Raised on class: lte.ENBEquipment	Severity: major Specific problem: SRIOSW FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1806 IK4306428

Alarm	Attributes	Applicable major release
Name: IK4306428 (11046) Type: processingErrorAlarm Package: lte.IK4306428 Raised on class: lte.ENBEquipment	Severity: major Specific problem: SRIOSW FAULT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1807 IK4306429

Alarm	Attributes	Applicable major release
Name: IK4306429 (11047) Type: processingErrorAlarm Package: lte.IK4306429 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: SRIOSW FAULT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1808 IK4306430

Alarm	Attributes	Applicable major release
Name: IK4306430 (11048) Type: processingErrorAlarm Package: lte.IK4306430 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SRIOSW EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: No action is required.		

Table 29-1809 IK4306431

Alarm	Attributes	Applicable major release
Name: IK4306431 (11049) Type: equipmentAlarm Package: lte.IK4306431 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SRIOSW EVENT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: No action is required.		

Table 29-1810 IK4306432

Alarm	Attributes	Applicable major release
Name: IK4306432 (11050) Type: processingErrorAlarm Package: lte.IK4306432 Raised on classes: • lte.CBCardSpecifics • lte.BBCardSpecifics	Severity: major Specific problem: CALLP DATA LOADING NOT FINISHED IN TIME Implicitly cleared: true Default probable cause: softwareError	Release: • LR16.1.L • LR16.2.L

Table 29-1810 IK4306432 (continued)

Alarm	Attributes	Applicable major release
Description: The CallP application was unable to load its configuration data in time.		
Remedial action: The impacted unit is automatically restarted. If the problem persists, reset the eNodeB.		

Table 29-1811 IK4500049

Alarm	Attributes	Applicable major release
Name: IK4500049 (8930) Type: equipmentAlarm Package: lte.IK4500049 Raised on class: lte.Rae	Severity: minor Specific problem: RAE ALD UNIT SUPPORT WRONG AISG VERSION Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RAE unit does not support AISG version 2.1.		
Remedial action: Upgrade the software.		

Table 29-1812 IK4500050

Alarm	Attributes	Applicable major release
Name: IK4500050 (8931) Type: equipmentAlarm Package: lte.IK4500050 Raised on class: lte.Rae	Severity: critical Specific problem: RAE LOSS OF COMM Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • LR15.1.L
Description: This alarm indicates the RFM that acts as an AISG Controller lost communication to the RAE unit.		
Remedial action: Inspect and repair the AISG bus if needed, otherwise replace the RAE.		

Table 29-1813 IK4500052

Alarm	Attributes	Applicable major release
Name: IK4500052 (8932) Type: equipmentAlarm Package: lte.IK4500052 Raised on class: lte.SFP	Severity: minor Specific problem: SFP FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1814 IK4500053

Alarm	Attributes	Applicable major release
Name: IK4500053 (8933) Type: equipmentAlarm Package: lte.IK4500053 Raised on class: lte.Rae	Severity: critical Specific problem: RAESUBUNIT 1 MOTOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RAE SUBUNIT 1 motor cannot move.		
Remedial action: Check for obstruction of antenna tilt mechanism, or replace failed RAE SUBUNIT 1 actuator.		

Table 29-1815 IK4500060

Alarm	Attributes	Applicable major release
Name: IK4500060 (8934) Type: equipmentAlarm Package: lte.IK4500060 Raised on class: lte.Rae	Severity: minor Specific problem: RAESUBUNIT 1 ACTUATOR JAM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that the RAESUBUNIT 1 actuator jam has been detected. No movement of the actuator, but movement of the motor was detected.		
Remedial action: Check for obstruction of antenna tilt mechanism. If no obstruction was found, the RAE unit might have to be replaced since a subunit cannot be replaced. .		

Table 29-1816 IK4500069

Alarm	Attributes	Applicable major release
Name: IK4500069 (8935) Type: equipmentAlarm Package: lte.IK4500069 Raised on class: lte.Rae	Severity: major Specific problem: RAESUBUNIT 1 NOT CALIBRATED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates that RAESUBUNIT 1 in the RAE device has not completed a calibration operation, or calibration data was lost		
Remedial action: Execute the RAESUBUNIT 1 calibration procedure.		

Table 29-1817 IK4500077

Alarm	Attributes	Applicable major release
Name: IK4500077 (8936) Type: equipmentAlarm Package: lte.IK4500077 Raised on class: lte.Rae	Severity: minor Specific problem: RAESUBUNIT 1 NOT CONFIGURED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L

Table 29-1817 IK4500077 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that this RAESUBUNIT does not have an antenna configuration file (ACF).		
Remedial action: Download a proper ACF to this RAESUBUNIT and execute the calibration.procedure if the RAESUBUNIT does not do it automatically.		

Table 29-1818 IK4500085

Alarm	Attributes	Applicable major release
Name: IK4500085 (8937) Type: equipmentAlarm Package: lte.IK4500085 Raised on class: lte.Rae	Severity: minor Specific problem: RAE HW FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a general hardware failure in the RAE unit..		
Remedial action: Reset the RAE, replace the RAE unit if the problem persists.		

Table 29-1819 IK4500086

Alarm	Attributes	Applicable major release
Name: IK4500086 (8938) Type: equipmentAlarm Package: lte.IK4500086 Raised on class: lte.Rae	Severity: minor Specific problem: RAESUBUNIT 1 ACTUATOR INTERFERENCE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates an actuator movement outside the control of the RAESUBUNIT 1. Probable cause is manual interference.		
Remedial action: Check the antenna panel for mechanical interference.		

Table 29-1820 IK4500096

Alarm	Attributes	Applicable major release
Name: IK4500096 (8939) Type: equipmentAlarm Package: lte.IK4500096 Raised on class: lte.Rae	Severity: major Specific problem: RAE SOFTWARE FAIL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L
Description: This alarm indicates a general RAE SW failure.		
Remedial action: Reset the RAE unit. If the problem persists then download new software to the RAE unit, otherwise replace the RAE if problem persists.		

Table 29-1821 IK4500097

Alarm	Attributes	Applicable major release
Name: IK4500097 (10236) Type: equipmentAlarm Package: lte.IK4500097 Raised on class: lte.Rae	Severity: major Specific problem: RAE INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that a failure of the RAE has been detected that cannot described by any specific alarm.		
Remedial action: The unit is automatically reset to attempt to clear the fault. If the problem persists then replace the RAE.		

Table 29-1822 IK4500098

Alarm	Attributes	Applicable major release
Name: IK4500098 (10237) Type: equipmentAlarm Package: lte.IK4500098 Raised on class: lte.Rae	Severity: major Specific problem: WEIGHTING FACTOR PARAMETER READ FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that there was a failure while trying to read data from the RAESUBUNIT.		
Remedial action: The unit might have to be replaced if the problem persists.		

Table 29-1823 IK4500099

Alarm	Attributes	Applicable major release
Name: IK4500099 (10238) Type: operationalViolation Package: lte.IK4500099 Raised on class: lte.Rae	Severity: major Specific problem: INVALID WEIGHTING FACTORS PARAMETER Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that OAM could not match the value specified in the parameter wfElectricalTiltValue or wfBroadcastBemawidthValue is not one of the values supported by the RAE unit to retrieve the Weighting Factors values that are used for Beamforming.		
Remedial action: The operator will have to set the correct value in these parameters. The values supported by the RaeSubunit are stored in the MIM parameters RaeSubunit::listOfElectricalTiltValues and RaeSubunit::listOfBeamwidthValues		

Table 29-1824 IK4500100

Alarm	Attributes	Applicable major release
Name: IK4500100 (10239) Type: equipmentAlarm Package: lte.IK4500100 Raised on class: lte.Rae	Severity: major Specific problem: WEIGHTING FACTOR FILE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This event indicates that the download of a Weighting Factor File to the RAESUBUNIT failed..		
Remedial action: The download should be repeated and if the problem persists, the unit might have to be replaced.		

Table 29-1825 IK4500101

Alarm	Attributes	Applicable major release
Name: IK4500101 (8940) Type: equipmentAlarm Package: lte.IK4500101 Raised on class: lte.SFP	Severity: major Specific problem: CPRI PORT FAILURE Implicitly cleared: true Default probable cause: inputOutputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNB failed to send/receive traffic through a CPRI port.		
Remedial action: The eNB CPRI port equipment shall be checked and the eNB controller board or the SFP will be replaced if necessary.		

Table 29-1826 IK4500104

Alarm	Attributes	Applicable major release
Name: IK4500104 (8941) Type: equipmentAlarm Package: lte.IK4500104 Raised on class: lte.SFP	Severity: warning Specific problem: SFP INCOMPATIBILITY CPRIPORT Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that the equipped SFP doesn't allow to achieve the maximum CPRI rate allowed by SW.		
Remedial action: The operator may update the SFP.		

Table 29-1827 IK4500106

Alarm	Attributes	Applicable major release
Name: IK4500106 (8942) Type: equipmentAlarm Package: lte.IK4500106 Raised on class: lte.SFP	Severity: minor Specific problem: CPRI PORT FAILURE MINOR Implicitly cleared: true Default probable cause: inputOutputDeviceError	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1827 IK4500106 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the CPRI port detected a signal quality problem or an issue at the far end.		
Remedial action: The eNB CPRI port equipment shall be checked at both ends and replaced if necessary. The fiber optic transmission network needs to be analyzed.		

Table 29-1828 IK4500109

Alarm	Attributes	Applicable major release
Name: IK4500109 (10240) Type: equipmentAlarm Package: lte.IK4500109 Raised on class: lte.Rae	Severity: minor Specific problem: RAE FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RAE fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1829 IK4500110

Alarm	Attributes	Applicable major release
Name: IK4500110 (10241) Type: equipmentAlarm Package: lte.IK4500110 Raised on class: lte.Rae	Severity: major Specific problem: RAE FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RAE fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1830 IK4500111

Alarm	Attributes	Applicable major release
Name: IK4500111 (10242) Type: equipmentAlarm Package: lte.IK4500111 Raised on class: lte.Rae	Severity: major Specific problem: RAE FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified RAE fault.		
Remedial action: Check the additional info for maintenance action details.		

Table 29-1831 IK4500112

Alarm	Attributes	Applicable major release
Name: IK4500112 (10243) Type: equipmentAlarm Package: lte.IK4500112 Raised on class: lte.SFP	Severity: minor Specific problem: SFP FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1832 IK4500113

Alarm	Attributes	Applicable major release
Name: IK4500113 (10244) Type: equipmentAlarm Package: lte.IK4500113 Raised on class: lte.SFP	Severity: major Specific problem: SFP FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: Check the additional information for maintenance action details.		

Table 29-1833 IK4500114

Alarm	Attributes	Applicable major release
Name: IK4500114 (10245) Type: equipmentAlarm Package: lte.IK4500114 Raised on class: lte.SFP	Severity: indeterminate Specific problem: SFP EVENT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: No action is required.		

Table 29-1834 IK4500115

Alarm	Attributes	Applicable major release
Name: IK4500115 (10246) Type: equipmentAlarm Package: lte.IK4500115 Raised on class: lte.SFP	Severity: indeterminate Specific problem: SFP EVENT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: No action is required.		

Table 29-1835 IK4500116

Alarm	Attributes	Applicable major release
Name: IK4500116 (10247) Type: equipmentAlarm Package: lte.IK4500116 Raised on class: lte.SFP	Severity: indeterminate Specific problem: SFP EVENT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. Unspecified SFP fault detected		
Remedial action: No action is required.		

Table 29-1836 IK4500135

Alarm	Attributes	Applicable major release
Name: IK4500135 (10248) Type: equipmentAlarm Package: lte.IK4500135 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: INIT FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only.\nIt indicates the SRIO Switch Box has failed to initialize.		
Remedial action: Reset the SRIO Switch Box. If the problem persists, replace the SRIO Switch Box.		

Table 29-1837 IK4500136

Alarm	Attributes	Applicable major release
Name: IK4500136 (10249) Type: equipmentAlarm Package: lte.IK4500136 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: INDETERMINATE OPERATIONAL FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates a failure on operations performed on the SRIO Switch Box.		
Remedial action: Reset the SRIO Switch Box. If the problem persists, call the next level of support.		

Table 29-1838 IK4500137

Alarm	Attributes	Applicable major release
Name: IK4500137 (10250) Type: equipmentAlarm Package: lte.IK4500137 Raised on class: lte.ENBEquipment	Severity: major Specific problem: OVER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates the SRIO Switch Box temperature is too high.		

Table 29-1838 IK4500137 (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check if the SRIO Switch Box Fan alarm is raised. Check the SRIO Switch Box FAN. Check the SRIO Switch Box air filter.		

Table 29-1839 IK4500138

Alarm	Attributes	Applicable major release
Name: IK4500138 (10251) Type: equipmentAlarm Package: lte.IK4500138 Raised on class: lte.ENBEquipment	Severity: major Specific problem: FAN ALARM MAJOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates that one or several fans of the SRIO Switch Box failed.		
Remedial action: Check the SRIO Switch Box fan. Replace it.		

Table 29-1840 IK4500140

Alarm	Attributes	Applicable major release
Name: IK4500140 (10253) Type: equipmentAlarm Package: lte.IK4500140 Raised on class: lte.ENBEquipment	Severity: major Specific problem: DC POWER FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only.\nIt indicates the SRIO Switch Box DC power failed.		
Remedial action: Check the SRIO Switch Box. if the problem persists, replace the SRIO Switch Box.		

Table 29-1841 IK4500141

Alarm	Attributes	Applicable major release
Name: IK4500141 (10254) Type: equipmentAlarm Package: lte.IK4500141 Raised on class: lte.ENBEquipment	Severity: critical Specific problem: LOSS OF COMM Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates the Ethernet communication with the SRIO Switch Box failed.\n.		
Remedial action: Check the SRIO Switch Box. If the problem persists, call the next level of support.		

Table 29-1842 IK4500142

Alarm	Attributes	Applicable major release
Name: IK4500142 (10255) Type: equipmentAlarm Package: lte.IK4500142 Raised on class: lte.ENBEquipment	Severity: major Specific problem: SRIO SWITCH FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates that the SRIO switch of the SRIO Switch Box failed.		
Remedial action: Check the SRIO Switch Box. Resets it. If the problem persists, replace the SRIO Switch Box.		

Table 29-1843 IK4500143

Alarm	Attributes	Applicable major release
Name: IK4500143 (10256) Type: equipmentAlarm Package: lte.IK4500143 Raised on class: lte.ENBEquipment	Severity: major Specific problem: ETHERNET SWITCH FAILED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates that the Ethernet switch of the SRIO Switch Box failed.		
Remedial action: Check the SRIO Switch Box. Resets it. If the problem persists, replace the SRIO Switch Box.		

Table 29-1844 IK4500144

Alarm	Attributes	Applicable major release
Name: IK4500144 (10257) Type: equipmentAlarm Package: lte.IK4500144 Raised on class: lte.ENBEquipment	Severity: minor Specific problem: ALD DEVICE NOT FOUND FOR SPECIFIED UNIQUE IDENTIFIER NUMBER Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm indicates that the eNodeB was not able to create the MIM object due to the missing HW.		
Remedial action: The Work Order should be checked to make sure that the ald unique name was entered correctly and/or that the ALD is actually part of the eNodeB..		

Table 29-1845 IK4500145

Alarm	Attributes	Applicable major release
Name: IK4500145 (10258) Type: equipmentAlarm Package: lte.IK4500145 Raised on class: lte.Rae	Severity: major Specific problem: WEIGHTING FACTORS MISSING IN RAE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L

Table 29-1845 IK4500145 (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicates that the eNodeB was not able to retrieve Weighting Factors from a RAE unit.		
Remedial action: Download the Weighting Factors File to the RAE unit.		

Table 29-1846 IK4500146

Alarm	Attributes	Applicable major release
Name: IK4500146 (10259) Type: equipmentAlarm Package: lte.IK4500146 Raised on class: lte.ENBEquipment	Severity: major Specific problem: UNDER TEMP CRITICAL Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates the SRIO Switch Box temperature is too low.		
Remedial action: Check if the SRIO Switch Box Fan alarm is raised. Check the SRIO Switch Box FAN. Check the SRIO Switch Box air filter.		

Table 29-1847 IK4500147

Alarm	Attributes	Applicable major release
Name: IK4500147 (10260) Type: equipmentAlarm Package: lte.IK4500147 Raised on class: lte.ENBEquipment	Severity: major Specific problem: INPUT VOLTAGE FAILURE Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: This alarm applies to hotel BBU configurations only. It indicates the SRIO Switch Box input voltage failed.		
Remedial action: Check the SRIO Switch Box. if the problem persists, replace the SRIO Switch Box.		

Table 29-1848 IK4500164

Alarm	Attributes	Applicable major release
Name: IK4500164 (11051) Type: equipmentAlarm Package: lte.IK4500164 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: MB FAULT 1 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1849 IK4500165

Alarm	Attributes	Applicable major release
Name: IK4500165 (11052) Type: equipmentAlarm Package: lte.IK4500165 Raised on class: lte.BBCardSpecifics	Severity: minor Specific problem: MB FAULT 2 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1850 IK4500166

Alarm	Attributes	Applicable major release
Name: IK4500166 (11053) Type: equipmentAlarm Package: lte.IK4500166 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: MB FAULT 3 Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1851 IK4500167

Alarm	Attributes	Applicable major release
Name: IK4500167 (11054) Type: equipmentAlarm Package: lte.IK4500167 Raised on class: lte.BBCardSpecifics	Severity: major Specific problem: MB FAULT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: Refer to additional information in the alarm report.		

Table 29-1852 IK4500168

Alarm	Attributes	Applicable major release
Name: IK4500168 (11055) Type: equipmentAlarm Package: lte.IK4500168 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MB EVENT 1 Implicitly cleared: true Default probable cause: unknown	Release: • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This is a spare alarm for future use.		
Remedial action: No action is required.		

Table 29-1853 IK4901001

Alarm	Attributes	Applicable major release
Name: IK4901001 (2761) Type: equipmentAlarm Package: lte.IK4901001 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: POWER ON Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system is powered on successfully.		
Remedial action: No action is required.		

Table 29-1854 IK4901002

Alarm	Attributes	Applicable major release
Name: IK4901002 (2762) Type: processingErrorAlarm Package: lte.IK4901002 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1855 IK4901003

Alarm	Attributes	Applicable major release
Name: IK4901003 (2763) Type: processingErrorAlarm Package: lte.IK4901003 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1856 IK4901004

Alarm	Attributes	Applicable major release
Name: IK4901004 (2764) Type: processingErrorAlarm Package: lte.IK4901004 Raised on class: lte.RRH	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1857 IK4901005

Alarm	Attributes	Applicable major release
Name: IK4901005 (2765) Type: processingErrorAlarm Package: lte.IK4901005 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1858 IK4901006

Alarm	Attributes	Applicable major release
Name: IK4901006 (2766) Type: equipmentAlarm Package: lte.IK4901006 Raised on class: lte.RFM	Severity: warning Specific problem: UNSUPPORTED DELEGATION BY OTHER CONTROLLER Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The primary controller for this RE (CDMA, WCDMA or GSM) has delegated a management function such as 'Software Management' to the LTE controller. This function is not supported by this LTE release.		
Remedial action: Reconfigure the RE on the primary controller (CDMA, WCDMA or GSM) to no longer delegate the unsupported management function to LTE.		

Table 29-1859 IK4901010

Alarm	Attributes	Applicable major release
Name: IK4901010 (2770) Type: equipmentAlarm Package: lte.IK4901010 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET OAM EXCEPTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller is reset due to an processor exception.		
Remedial action: No action is required.		

Table 29-1860 IK4901011

Alarm	Attributes	Applicable major release
Name: IK4901011 (2771) Type: equipmentAlarm Package: lte.IK4901011 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation and the successful data migration.		
Remedial action: No action is required.		

Table 29-1861 IK4901012

Alarm	Attributes	Applicable major release
Name: IK4901012 (2772) Type: equipmentAlarm Package: lte.IK4901012 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITHOUT DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation without a data migration.		
Remedial action: No action is required.		

Table 29-1862 IK4901013

Alarm	Attributes	Applicable major release
Name: IK4901013 (2773) Type: equipmentAlarm Package: lte.IK4901013 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation. The database is not found.		
Remedial action: No action is required.		

Table 29-1863 IK4901014

Alarm	Attributes	Applicable major release
Name: IK4901014 (2774) Type: equipmentAlarm Package: lte.IK4901014 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET AFTER REJECT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1863 IK4901014 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version.		
Remedial action: No action is required.		

Table 29-1864 IK4901015

Alarm	Attributes	Applicable major release
Name: IK4901015 (2775) Type: equipmentAlarm Package: lte.IK4901015 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET AFTER REJECT WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version. The database is not found.		
Remedial action: No action is required.		

Table 29-1865 IK4901016

Alarm	Attributes	Applicable major release
Name: IK4901016 (2776) Type: equipmentAlarm Package: lte.IK4901016 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: AUTO-REJECT TO PREVIOUS SW VERSION AFTER ACTIVATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a reset was performed due to the activation of the previous software version caused by a corrupt file.		
Remedial action: No action is required.		

Table 29-1866 IK4901018

Alarm	Attributes	Applicable major release
Name: IK4901018 (2778) Type: equipmentAlarm Package: lte.IK4901018 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: SW UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the board was enabled with invalid software. OAM automatically updates the required software version.		
Remedial action: No action is required.		

Table 29-1867 IK4901019

Alarm	Attributes	Applicable major release
Name: IK4901019 (2779) Type: equipmentAlarm Package: lte.IK4901019 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure of the FTP transfer of the software package from the code-server to the local RAM disk.		
Remedial action: No action is required.		

Table 29-1868 IK4901020

Alarm	Attributes	Applicable major release
Name: IK4901020 (2780) Type: equipmentAlarm Package: lte.IK4901020 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CB MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1869 IK4901022

Alarm	Attributes	Applicable major release
Name: IK4901022 (2782) Type: equipmentAlarm Package: lte.IK4901022 Raised on class: lte.RRH	Severity: indeterminate Specific problem: RRH MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1870 IK4901023

Alarm	Attributes	Applicable major release
Name: IK4901023 (2783) Type: equipmentAlarm Package: lte.IK4901023 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: TRDU MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1870 IK4901023 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1871 IK4901024

Alarm	Attributes	Applicable major release
Name: IK4901024 (2784) Type: equipmentAlarm Package: lte.IK4901024 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: SOFTWARE AND DATABASE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1872 IK4901025

Alarm	Attributes	Applicable major release
Name: IK4901025 (2785) Type: equipmentAlarm Package: lte.IK4901025 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: SOFTWARE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1873 IK4901026

Alarm	Attributes	Applicable major release
Name: IK4901026 (2786) Type: equipmentAlarm Package: lte.IK4901026 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: NEW SW DOES NOT SUPPORT ALL ACTUAL HW MODULES Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the new software package does not support all actual hardware modules installed in the eNodeB.		
Remedial action: No action is required.		

Table 29-1874 IK4901027

Alarm	Attributes	Applicable major release
Name: IK4901027 (3274) Type: equipmentAlarm Package: lte.IK4901027 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BACK TO FACTORY MODE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that software meta data is deleted or corrupted.		
Remedial action: No action is required.		

Table 29-1875 IK4901028

Alarm	Attributes	Applicable major release
Name: IK4901028 (3275) Type: equipmentAlarm Package: lte.IK4901028 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BACK TO MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1876 IK4901029

Alarm	Attributes	Applicable major release
Name: IK4901029 (3276) Type: equipmentAlarm Package: lte.IK4901029 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BACK TO FACTORY MODE AND MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that software meta data is deleted or corrupted and that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1877 IK4901030

Alarm	Attributes	Applicable major release
Name: IK4901030 (3277) Type: equipmentAlarm Package: lte.IK4901030 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: BB MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		

Table 29-1877 IK4901030 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1878 IK4901031

Alarm	Attributes	Applicable major release
Name: IK4901031 (3278) Type: equipmentAlarm Package: lte.IK4901031 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET CONTROLLER OAM LACK RESOURCE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller board is reset due to lack of internal resources.		
Remedial action: No action is required.		

Table 29-1879 IK4901032

Alarm	Attributes	Applicable major release
Name: IK4901032 (3279) Type: equipmentAlarm Package: lte.IK4901032 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET CONTROLLER WATCHDOG Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller is reset due to hardware watchdog timeout.		
Remedial action: No action is required.		

Table 29-1880 IK4901033

Alarm	Attributes	Applicable major release
Name: IK4901033 (3280) Type: equipmentAlarm Package: lte.IK4901033 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CONTROLLER OAM AUTO RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller is auto-reset due to an internal problem.		
Remedial action: No action is required.		

Table 29-1881 IK4901034

Alarm	Attributes	Applicable major release
Name: IK4901034 (3281) Type: equipmentAlarm Package: lte.IK4901034 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: OAM AUTO RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates an OAM auto-reset due to an internal problem.		
Remedial action: No action is required.		

Table 29-1882 IK4901035

Alarm	Attributes	Applicable major release
Name: IK4901035 (3854) Type: equipmentAlarm Package: lte.IK4901035 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: UNEXPECTED CONTROL BOARD RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the control board suffered from an unexpected, unplanned reset.\nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1883 IK4901036

Alarm	Attributes	Applicable major release
Name: IK4901036 (4121) Type: equipmentAlarm Package: lte.IK4901036 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: AUTO-REJECT TO PREVIOUS SW VERSION AFTER ACTIVATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a reset was performed due to the activation of the previous software version caused by a corrupt file.		
Remedial action: No action is required.		

Table 29-1884 IK4901037

Alarm	Attributes	Applicable major release
Name: IK4901037 (4122) Type: equipmentAlarm Package: lte.IK4901037 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BACK TO FACTORY MODE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that software meta data is deleted or corrupted.		
Remedial action: No action is required.		

Table 29-1885 IK4901038

Alarm	Attributes	Applicable major release
Name: IK4901038 (4123) Type: equipmentAlarm Package: lte.IK4901038 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BACK TO MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1886 IK4901039

Alarm	Attributes	Applicable major release
Name: IK4901039 (4124) Type: equipmentAlarm Package: lte.IK4901039 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BACK TO FACTORY MODE AND MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that software meta data is deleted or corrupted and that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1887 IK4901040

Alarm	Attributes	Applicable major release
Name: IK4901040 (4125) Type: equipmentAlarm Package: lte.IK4901040 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure of the FTP transfer of the software package from the code-server to the local RAM disk.		

Table 29-1887 IK4901040 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1888 IK4901041

Alarm	Attributes	Applicable major release
Name: IK4901041 (4126) Type: equipmentAlarm Package: lte.IK4901041 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SCB MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1889 IK4901042

Alarm	Attributes	Applicable major release
Name: IK4901042 (4127) Type: equipmentAlarm Package: lte.IK4901042 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: CONTROLLER OAM AUTO RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller is auto-reset due to an internal problem.		
Remedial action: No action is required.		

Table 29-1890 IK4901043

Alarm	Attributes	Applicable major release
Name: IK4901043 (4128) Type: processingErrorAlarm Package: lte.IK4901043 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1891 IK4901044

Alarm	Attributes	Applicable major release
Name: IK4901044 (4129) Type: equipmentAlarm Package: lte.IK4901044 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: NEW SW DOES NOT SUPPORT ALL ACTUAL HW MODULES Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the new software package does not support all actual hardware modules installed in the eNodeB.		
Remedial action: No action is required.		

Table 29-1892 IK4901045

Alarm	Attributes	Applicable major release
Name: IK4901045 (4130) Type: equipmentAlarm Package: lte.IK4901045 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: OAM AUTO RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates an OAM auto-reset due to an internal problem.		
Remedial action: No action is required.		

Table 29-1893 IK4901046

Alarm	Attributes	Applicable major release
Name: IK4901046 (4131) Type: equipmentAlarm Package: lte.IK4901046 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: POWER ON Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the system is powered on successfully.		
Remedial action: No action is required.		

Table 29-1894 IK4901047

Alarm	Attributes	Applicable major release
Name: IK4901047 (4132) Type: equipmentAlarm Package: lte.IK4901047 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation and the successful data migration.		

Table 29-1894 IK4901047 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1895 IK4901048

Alarm	Attributes	Applicable major release
Name: IK4901048 (4133) Type: equipmentAlarm Package: lte.IK4901048 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITHOUT DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation without a data migration.		
Remedial action: No action is required.		

Table 29-1896 IK4901049

Alarm	Attributes	Applicable major release
Name: IK4901049 (4134) Type: equipmentAlarm Package: lte.IK4901049 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the software activation. The database is not found.		
Remedial action: No action is required.		

Table 29-1897 IK4901050

Alarm	Attributes	Applicable major release
Name: IK4901050 (4135) Type: equipmentAlarm Package: lte.IK4901050 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER REJECT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version.		
Remedial action: No action is required.		

Table 29-1898 IK4901051

Alarm	Attributes	Applicable major release
Name: IK4901051 (4136) Type: equipmentAlarm Package: lte.IK4901051 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER REJECT WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version. The database is not found.		
Remedial action: No action is required.		

Table 29-1899 IK4901052

Alarm	Attributes	Applicable major release
Name: IK4901052 (4137) Type: equipmentAlarm Package: lte.IK4901052 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER OAM LACK RESOURCE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller board is reset due to lack of internal resources.		
Remedial action: No action is required.		

Table 29-1900 IK4901053

Alarm	Attributes	Applicable major release
Name: IK4901053 (4138) Type: equipmentAlarm Package: lte.IK4901053 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER WATCHDOG Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller is reset due to hardware watchdog timeout.		
Remedial action: No action is required.		

Table 29-1901 IK4901054

Alarm	Attributes	Applicable major release
Name: IK4901054 (4139) Type: equipmentAlarm Package: lte.IK4901054 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET OAM EXCEPTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1901 IK4901054 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the controller is reset due to an processor exception.		
Remedial action: No action is required.		

Table 29-1902 IK4901055

Alarm	Attributes	Applicable major release
Name: IK4901055 (4140) Type: equipmentAlarm Package: lte.IK4901055 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SOFTWARE AND DATABASE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1903 IK4901056

Alarm	Attributes	Applicable major release
Name: IK4901056 (4141) Type: equipmentAlarm Package: lte.IK4901056 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SOFTWARE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1904 IK4901057

Alarm	Attributes	Applicable major release
Name: IK4901057 (4142) Type: equipmentAlarm Package: lte.IK4901057 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: SW UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the board was enabled with invalid software. OAM automatically updates the required software version.		
Remedial action: No action is required.		

Table 29-1905 IK4901058

Alarm	Attributes	Applicable major release
Name: IK4901058 (4143) Type: equipmentAlarm Package: lte.IK4901058 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: UNEXPECTED CONTROL BOARD RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the control board suffered from an unexpected, unplanned reset. \nMore detailed information on the cause of this event is included in the Additional Information section of the event. This section provides detailed failure information intended for Nokia support and R&D experts to allow them to identify unique fault signatures of eNodeB hardware and software problems. \nThe information provided here is generally called a Fault Signature. The fault signature provides the raw material that can be used to diagnose a root cause for the event. It does not directly provide the root cause, but rather portions of a signature of a fault that can be compared to other faults. Each fault is different, but a unique fault signature can be constructed using combinations of data in the events.\n\nFor a description of eNodeB Fault Signatures included in failure events, see 'Fault Signatures for bCEM, eCCM and Cell failure Events' (p. 1-9). Contact Nokia support for further assistance.		
Remedial action: No action is required.		

Table 29-1906 IK4901059

Alarm	Attributes	Applicable major release
Name: IK4901059 (4144) Type: processingErrorAlarm Package: lte.IK4901059 Raised on class: lte.RFME	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1907 IK4901060

Alarm	Attributes	Applicable major release
Name: IK4901060 (4145) Type: equipmentAlarm Package: lte.IK4901060 Raised on class: lte.RFME	Severity: indeterminate Specific problem: RFME MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1908 IK4901062

Alarm	Attributes	Applicable major release
Name: IK4901062 (8943) Type: equipmentAlarm Package: lte.IK4901062 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET DUE TO LOCKED DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB is reset due to an unrecoverable Database lock		
Remedial action: No action is required.		

Table 29-1909 IK4901064

Alarm	Attributes	Applicable major release
Name: IK4901064 (8944) Type: equipmentAlarm Package: lte.IK4901064 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: OAM AUTO RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates an OAM auto-reset due to an internal problem.		
Remedial action: No action is required.		

Table 29-1910 IK4901065

Alarm	Attributes	Applicable major release
Name: IK4901065 (8945) Type: equipmentAlarm Package: lte.IK4901065 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER WATCHDOG Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the controller is reset due to hardware watchdog timeout.		
Remedial action: No action is required.		

Table 29-1911 IK4901066

Alarm	Attributes	Applicable major release
Name: IK4901066 (8946) Type: equipmentAlarm Package: lte.IK4901066 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER OAM LACK RESOURCE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the controller board is reset due to lack of internal resources.		
Remedial action: No action is required.		

Table 29-1912 IK4901067

Alarm	Attributes	Applicable major release
Name: IK4901067 (8947) Type: equipmentAlarm Package: lte.IK4901067 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BACK TO MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1913 IK4901068

Alarm	Attributes	Applicable major release
Name: IK4901068 (8948) Type: equipmentAlarm Package: lte.IK4901068 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BACK TO FACTORY MODE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that software meta data is deleted or corrupted.		
Remedial action: No action is required.		

Table 29-1914 IK4901069

Alarm	Attributes	Applicable major release
Name: IK4901069 (8949) Type: equipmentAlarm Package: lte.IK4901069 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: BACK TO FACTORY MODE AND MINIMUM DB Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that software meta data is deleted or corrupted and that the database contents have been reset to default.		
Remedial action: No action is required.		

Table 29-1915 IK4901070

Alarm	Attributes	Applicable major release
Name: IK4901070 (8950) Type: equipmentAlarm Package: lte.IK4901070 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: NEW SW DOES NOT SUPPORT ALL ACTUAL HW MODULES Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the new software package does not support all actual hardware modules installed in the eNodeB.		
Remedial action: No action is required.		

Table 29-1916 IK4901071

Alarm	Attributes	Applicable major release
Name: IK4901071 (8951) Type: equipmentAlarm Package: lte.IK4901071 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: SOFTWARE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1917 IK4901072

Alarm	Attributes	Applicable major release
Name: IK4901072 (8952) Type: equipmentAlarm Package: lte.IK4901072 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: SOFTWARE AND DATABASE FALLBACK Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB has detected a critical failure during eNodeB initialization while booting from the active software partition. The eNodeB has switched over to the passive software partition and booted up on the previous software version with the previous configuration data.		
Remedial action: No action is required.		

Table 29-1918 IK4901073

Alarm	Attributes	Applicable major release
Name: IK4901073 (8953) Type: equipmentAlarm Package: lte.IK4901073 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.RRH	Severity: indeterminate Specific problem: MODULE DOWNLOAD FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to transfer the software package from the local storage to the board.		
Remedial action: No action is required.		

Table 29-1919 IK4901074

Alarm	Attributes	Applicable major release
Name: IK4901074 (8954) Type: equipmentAlarm Package: lte.IK4901074 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: SW UPDATED AUTOMATICALLY Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the board was enabled with invalid software. OAM automatically updates the required software version.		

Table 29-1919 IK4901074 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1920 IK4901075

Alarm	Attributes	Applicable major release
Name: IK4901075 (8955) Type: equipmentAlarm Package: lte.IK4901075 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: AUTO-REJECT TO PREVIOUS SW VERSION AFTER ACTIVATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a reset was performed due to the activation of the previous software version caused by a corrupt file.		
Remedial action: No action is required.		

Table 29-1921 IK4901076

Alarm	Attributes	Applicable major release
Name: IK4901076 (8956) Type: equipmentAlarm Package: lte.IK4901076 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER REJECT WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version. The database is not found.		
Remedial action: No action is required.		

Table 29-1922 IK4901077

Alarm	Attributes	Applicable major release
Name: IK4901077 (8957) Type: equipmentAlarm Package: lte.IK4901077 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER REJECT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1922 IK4901077 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the software is rejected. The module is reset to activate the previous software version.		
Remedial action: No action is required.		

Table 29-1923 IK4901078

Alarm	Attributes	Applicable major release
Name: IK4901078 (8958) Type: equipmentAlarm Package: lte.IK4901078 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the software activation. The database is not found.		
Remedial action: No action is required.		

Table 29-1924 IK4901079

Alarm	Attributes	Applicable major release
Name: IK4901079 (8959) Type: equipmentAlarm Package: lte.IK4901079 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITHOUT DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the software activation without a data migration.		
Remedial action: No action is required.		

Table 29-1925 IK4901080

Alarm	Attributes	Applicable major release
Name: IK4901080 (8960) Type: equipmentAlarm Package: lte.IK4901080 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET AFTER ACTIVATE WITH DB MIGRATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-1925 IK4901080 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates the software activation and the successful data migration.		
Remedial action: No action is required.		

Table 29-1926 IK4901081

Alarm	Attributes	Applicable major release
Name: IK4901081 (8961) Type: equipmentAlarm Package: lte.IK4901081 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: RESET OAM EXCEPTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the controller is reset due to an processor exception.		
Remedial action: No action is required.		

Table 29-1927 IK4901082

Alarm	Attributes	Applicable major release
Name: IK4901082 (8962) Type: processingErrorAlarm Package: lte.IK4901082 Raised on classes: • lte.CBCardSpecifics • lte.RFME • lte.BBCardSpecifics • lte.TRDU • lte.MODULE • lte.RRH	Severity: indeterminate Specific problem: CORRUPT FILE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a checksum error.		
Remedial action: No action is required.		

Table 29-1928 IK4901083

Alarm	Attributes	Applicable major release
Name: IK4901083 (8963) Type: equipmentAlarm Package: lte.IK4901083 Raised on classes: • lte.CBCardSpecifics • lte.MODULE	Severity: indeterminate Specific problem: POWER ON Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the system is powered on successfully.		
Remedial action: No action is required.		

Table 29-1929 IK4904001

Alarm	Attributes	Applicable major release
Name: IK4904001 (2787) Type: equipmentAlarm Package: lte.IK4904001 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1930 IK4904002

Alarm	Attributes	Applicable major release
Name: IK4904002 (2788) Type: equipmentAlarm Package: lte.IK4904002 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1931 IK4904003

Alarm	Attributes	Applicable major release
Name: IK4904003 (2789) Type: equipmentAlarm Package: lte.IK4904003 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1931 IK4904003 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1932 IK4904004

Alarm	Attributes	Applicable major release
Name: IK4904004 (2790) Type: equipmentAlarm Package: lte.IK4904004 Raised on class: lte.RRH	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1933 IK4904005

Alarm	Attributes	Applicable major release
Name: IK4904005 (2791) Type: equipmentAlarm Package: lte.IK4904005 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1934 IK4904006

Alarm	Attributes	Applicable major release
Name: IK4904006 (2792) Type: processingErrorAlarm Package: lte.IK4904006 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1935 IK4904007

Alarm	Attributes	Applicable major release
Name: IK4904007 (2793) Type: processingErrorAlarm Package: lte.IK4904007 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1936 IK4904008

Alarm	Attributes	Applicable major release
Name: IK4904008 (2794) Type: processingErrorAlarm Package: lte.IK4904008 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1937 IK4904011

Alarm	Attributes	Applicable major release
Name: IK4904011 (2795) Type: processingErrorAlarm Package: lte.IK4904011 Raised on class: lte.RRH	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1938 IK4904013

Alarm	Attributes	Applicable major release
Name: IK4904013 (2796) Type: processingErrorAlarm Package: lte.IK4904013 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1939 IK4904016

Alarm	Attributes	Applicable major release
Name: IK4904016 (2797) Type: equipmentAlarm Package: lte.IK4904016 Raised on class: lte.RRH	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-1940 IK4904017

Alarm	Attributes	Applicable major release
Name: IK4904017 (2798) Type: equipmentAlarm Package: lte.IK4904017 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-1941 IK4904018

Alarm	Attributes	Applicable major release
Name: IK4904018 (2799) Type: equipmentAlarm Package: lte.IK4904018 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-1942 IK4904019

Alarm	Attributes	Applicable major release
Name: IK4904019 (2800) Type: qualityOfServiceAlarm Package: lte.IK4904019 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SNAPSHOT FILE AVAILABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the availability of new snapshot files.		
Remedial action: No action is required.		

Table 29-1943 IK4904020

Alarm	Attributes	Applicable major release
Name: IK4904020 (2801) Type: qualityOfServiceAlarm Package: lte.IK4904020 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: POSTMORTEM FILE AVAILABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the availability of new post-mortem files.		
Remedial action: No action is required.		

Table 29-1944 IK4904021

Alarm	Attributes	Applicable major release
Name: IK4904021 (2802) Type: qualityOfServiceAlarm Package: lte.IK4904021 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SNAPSHOT FILE FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the transfer of the new snapshot files to the target server failed.		
Remedial action: No action is required.		

Table 29-1945 IK4904022

Alarm	Attributes	Applicable major release
Name: IK4904022 (2803) Type: qualityOfServiceAlarm Package: lte.IK4904022 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: POSTMORTEM FILE FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the transfer of new post-mortem files to the target server failed.		
Remedial action: No action is required.		

Table 29-1946 IK4904023

Alarm	Attributes	Applicable major release
Name: IK4904023 (2804) Type: equipmentAlarm Package: lte.IK4904023 Raised on class: lte.AMR	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		

Table 29-1946 IK4904023 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1947 IK4904024

Alarm	Attributes	Applicable major release
Name: IK4904024 (2805) Type: equipmentAlarm Package: lte.IK4904024 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-1948 IK4904025

Alarm	Attributes	Applicable major release
Name: IK4904025 (2806) Type: equipmentAlarm Package: lte.IK4904025 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: MODULE INSERTION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a module insertion.		
Remedial action: No action is required.		

Table 29-1949 IK4904026

Alarm	Attributes	Applicable major release
Name: IK4904026 (2807) Type: processingErrorAlarm Package: lte.IK4904026 Raised on class: lte.AMR	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1950 IK4904027

Alarm	Attributes	Applicable major release
Name: IK4904027 (2808) Type: processingErrorAlarm Package: lte.IK4904027 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1951 IK4904028

Alarm	Attributes	Applicable major release
Name: IK4904028 (2809) Type: processingErrorAlarm Package: lte.IK4904028 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1952 IK4904029

Alarm	Attributes	Applicable major release
Name: IK4904029 (3282) Type: processingErrorAlarm Package: lte.IK4904029 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: PROCESSING UNIT OCCUPANCY OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the processing unit is overloaded.		
Remedial action: No action is required.		

Table 29-1953 IK4904030

Alarm	Attributes	Applicable major release
Name: IK4904030 (3283) Type: processingErrorAlarm Package: lte.IK4904030 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RAM USAGE OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the RAM exhausted.		
Remedial action: No action is required.		

Table 29-1954 IK4904031

Alarm	Attributes	Applicable major release
Name: IK4904031 (3284) Type: processingErrorAlarm Package: lte.IK4904031 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: PROCESSING UNIT OCCUPANCY OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the processing unit is overloaded.		
Remedial action: No action is required.		

Table 29-1955 IK4904032

Alarm	Attributes	Applicable major release
Name: IK4904032 (3285) Type: processingErrorAlarm Package: lte.IK4904032 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: RAM USAGE OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the RAM exhausted.		
Remedial action: No action is required.		

Table 29-1956 IK4904033

Alarm	Attributes	Applicable major release
Name: IK4904033 (3286) Type: qualityOfServiceAlarm Package: lte.IK4904033 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT FILE AVAILABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the availability of new on-demand snapshot files.		
Remedial action: No action is required.		

Table 29-1957 IK4904034

Alarm	Attributes	Applicable major release
Name: IK4904034 (3287) Type: qualityOfServiceAlarm Package: lte.IK4904034 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT UPLOAD FAILED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1957 IK4904034 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that the transfer of the new on-demand snapshot files to the target server failed.		
Remedial action: No action is required.		

Table 29-1958 IK4904035

Alarm	Attributes	Applicable major release
Name: IK4904035 (3674) Type: qualityOfServiceAlarm Package: lte.IK4904035 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1959 IK4904036

Alarm	Attributes	Applicable major release
Name: IK4904036 (3855) Type: qualityOfServiceAlarm Package: lte.IK4904036 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1960 IK4904037

Alarm	Attributes	Applicable major release
Name: IK4904037 (3856) Type: qualityOfServiceAlarm Package: lte.IK4904037 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1961 IK4904038

Alarm	Attributes	Applicable major release
Name: IK4904038 (3857) Type: qualityOfServiceAlarm Package: lte.IK4904038 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1962 IK4904039

Alarm	Attributes	Applicable major release
Name: IK4904039 (3858) Type: qualityOfServiceAlarm Package: lte.IK4904039 Raised on class: lte.RRH	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1963 IK4904040

Alarm	Attributes	Applicable major release
Name: IK4904040 (4146) Type: qualityOfServiceAlarm Package: lte.IK4904040 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1964 IK4904041

Alarm	Attributes	Applicable major release
Name: IK4904041 (4147) Type: processingErrorAlarm Package: lte.IK4904041 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1964 IK4904041 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1965 IK4904042

Alarm	Attributes	Applicable major release
Name: IK4904042 (4148) Type: processingErrorAlarm Package: lte.IK4904042 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: PROCESSING UNIT OCCUPANCY OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This events indicates that the processing unit is overloaded.		
Remedial action: No action is required.		

Table 29-1966 IK4904043

Alarm	Attributes	Applicable major release
Name: IK4904043 (4149) Type: processingErrorAlarm Package: lte.IK4904043 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RAM USAGE OVERLOAD Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This events indicates that the RAM exhausted.		
Remedial action: No action is required.		

Table 29-1967 IK4904044

Alarm	Attributes	Applicable major release
Name: IK4904044 (4150) Type: equipmentAlarm Package: lte.IK4904044 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1968 IK4904045

Alarm	Attributes	Applicable major release
Name: IK4904045 (4151) Type: processingErrorAlarm Package: lte.IK4904045 Raised on class: lte.RFME	Severity: indeterminate Specific problem: CONFIGURATION TIMEOUT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the time-out for a response from the module.		
Remedial action: No action is required.		

Table 29-1969 IK4904046

Alarm	Attributes	Applicable major release
Name: IK4904046 (4152) Type: qualityOfServiceAlarm Package: lte.IK4904046 Raised on class: lte.RFME	Severity: indeterminate Specific problem: ALU DEBUG SESSION ON-DEMAND SNAPSHOT INTERNAL FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the on-demand snapshot request failed due to eNodeB internal error.		
Remedial action: No action is required.		

Table 29-1970 IK4904047

Alarm	Attributes	Applicable major release
Name: IK4904047 (4785) Type: equipmentAlarm Package: lte.IK4904047 Raised on class: lte.RFME	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1971 IK4904048

Alarm	Attributes	Applicable major release
Name: IK4904048 (4786) Type: equipmentAlarm Package: lte.IK4904048 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: UPDATE RI FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the failure to update the remote inventory information for the module.		
Remedial action: No action is required.		

Table 29-1972 IK4905002

Alarm	Attributes	Applicable major release
Name: IK4905002 (2811) Type: equipmentAlarm Package: lte.IK4905002 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET OAM ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1973 IK4905006

Alarm	Attributes	Applicable major release
Name: IK4905006 (2815) Type: equipmentAlarm Package: lte.IK4905006 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1974 IK4905007

Alarm	Attributes	Applicable major release
Name: IK4905007 (2816) Type: equipmentAlarm Package: lte.IK4905007 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1975 IK4905008

Alarm	Attributes	Applicable major release
Name: IK4905008 (2817) Type: equipmentAlarm Package: lte.IK4905008 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1976 IK4905009

Alarm	Attributes	Applicable major release
Name: IK4905009 (2818) Type: equipmentAlarm Package: lte.IK4905009 Raised on class: lte.RRH	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1977 IK4905010

Alarm	Attributes	Applicable major release
Name: IK4905010 (2819) Type: equipmentAlarm Package: lte.IK4905010 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1978 IK4905011

Alarm	Attributes	Applicable major release
Name: IK4905011 (2820) Type: equipmentAlarm Package: lte.IK4905011 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1979 IK4905012

Alarm	Attributes	Applicable major release
Name: IK4905012 (2821) Type: equipmentAlarm Package: lte.IK4905012 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1980 IK4905013

Alarm	Attributes	Applicable major release
Name: IK4905013 (2822) Type: equipmentAlarm Package: lte.IK4905013 Raised on class: lte.ENBShelfSpecifics	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1981 IK4905014

Alarm	Attributes	Applicable major release
Name: IK4905014 (2823) Type: equipmentAlarm Package: lte.IK4905014 Raised on class: lte.RRH	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1982 IK4905015

Alarm	Attributes	Applicable major release
Name: IK4905015 (2824) Type: equipmentAlarm Package: lte.IK4905015 Raised on class: lte.TRDU	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1983 IK4905016

Alarm	Attributes	Applicable major release
Name: IK4905016 (2825) Type: equipmentAlarm Package: lte.IK4905016 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1984 IK4905020

Alarm	Attributes	Applicable major release
Name: IK4905020 (2828) Type: communicationsAlarm Package: lte.IK4905020 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: DATABASE RECONFIGURATION RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a reset was performed due to a database reconfiguration.		
Remedial action: No action is required.		

Table 29-1985 IK4905022

Alarm	Attributes	Applicable major release
Name: IK4905022 (2830) Type: equipmentAlarm Package: lte.IK4905022 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: FALLBACK AFTER RECONFIGU-RATION Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the eNodeB did an autonomous fallback to the previous configuration because the contact to the network management system could not be restored.		
Remedial action: No action is required.		

Table 29-1986 IK4905023

Alarm	Attributes	Applicable major release
Name: IK4905023 (3288) Type: communicationsAlarm Package: lte.IK4905023 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: MAX NUMBER OF CARDINALITY REACHED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the maximum number of object cardinality is reached. The automatic creation of new objects is not possible anymore.		
Remedial action: No action is required.		

Table 29-1987 IK4905024

Alarm	Attributes	Applicable major release
Name: IK4905024 (3289) Type: equipmentAlarm Package: lte.IK4905024 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: RESET ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1988 IK4905025

Alarm	Attributes	Applicable major release
Name: IK4905025 (3290) Type: equipmentAlarm Package: lte.IK4905025 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: RESET CONTROLLER OAM ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-1989 IK4905026

Alarm	Attributes	Applicable major release
Name: IK4905026 (3291) Type: equipmentAlarm Package: lte.IK4905026 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller board is reset to restore the configuration data.		
Remedial action: No action is required.		

Table 29-1990 IK4905027

Alarm	Attributes	Applicable major release
Name: IK4905027 (3292) Type: equipmentAlarm Package: lte.IK4905027 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-1990 IK4905027 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates an OAM auto-reset with an empty database as the database was not restored properly.		
Remedial action: No action is required.		

Table 29-1991 IK4905028

Alarm	Attributes	Applicable major release
Name: IK4905028 (3293) Type: equipmentAlarm Package: lte.IK4905028 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BBU POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BBU position coordinates have changed. The GPS antenna of the eNodeB has been moved or the bbuPositionDeltaX/Y/Z coordinates have been reconfigured.		
Remedial action: No action is required.		

Table 29-1992 IK4905029

Alarm	Attributes	Applicable major release
Name: IK4905029 (3294) Type: equipmentAlarm Package: lte.IK4905029 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: BBU POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BBU position coordinates might not be correct.		
Remedial action: No action is required.		

Table 29-1993 IK4905030

Alarm	Attributes	Applicable major release
Name: IK4905030 (3295) Type: equipmentAlarm Package: lte.IK4905030 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the main RF antenna position coordinates have changed. The GPS antenna of the eNodeB has been moved or the mainAntennaPositionDeltaX/Y/Z values have been reconfigured.		
Remedial action: No action is required.		

Table 29-1994 IK4905031

Alarm	Attributes	Applicable major release
Name: IK4905031 (3296) Type: equipmentAlarm Package: lte.IK4905031 Raised on class: lte.CBCardSpecifics	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the main RF antenna position coordinates might not be correct.		
Remedial action: No action is required.		

Table 29-1995 IK4905035

Alarm	Attributes	Applicable major release
Name: IK4905035 (3300) Type: processingErrorAlarm Package: lte.IK4905035 Raised on class: lte.Cell	Severity: indeterminate Specific problem: OAM CELL EVENT 4 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This event is for future use.		
Remedial action: No action is required.		

Table 29-1996 IK4905036

Alarm	Attributes	Applicable major release
Name: IK4905036 (3301) Type: processingErrorAlarm Package: lte.IK4905036 Raised on class: lte.Cell	Severity: indeterminate Specific problem: OAM CELL EVENT 5 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This event is for future use.		
Remedial action: No action is required.		

Table 29-1997 IK4905037

Alarm	Attributes	Applicable major release
Name: IK4905037 (3675) Type: equipmentAlarm Package: lte.IK4905037 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		

Table 29-1997 IK4905037 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-1998 IK4905038

Alarm	Attributes	Applicable major release
Name: IK4905038 (3676) Type: equipmentAlarm Package: lte.IK4905038 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-1999 IK4905039

Alarm	Attributes	Applicable major release
Name: IK4905039 (3677) Type: equipmentAlarm Package: lte.IK4905039 Raised on class: lte.TmaAldEntry	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2000 IK4905040

Alarm	Attributes	Applicable major release
Name: IK4905040 (3678) Type: equipmentAlarm Package: lte.IK4905040 Raised on class: lte.RetAldEntry	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2001 IK4905041

Alarm	Attributes	Applicable major release
Name: IK4905041 (3679) Type: equipmentAlarm Package: lte.IK4905041 Raised on class: lte.RFM	Severity: indeterminate Specific problem: CELL BLOCK REQUEST RECEIVED AT SHARED RFM Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the RFM is about to interrupt RF operation and so any cells fully supported on the RFM should be blocked. This cell block procedure is supported on shared RFMs (including ROCM) and is triggered by the other controller sharing the RFM.		
Remedial action: No action is required.		

Table 29-2002 IK4905044

Alarm	Attributes	Applicable major release
Name: IK4905044 (3860) Type: communicationsAlarm Package: lte.IK4905044 Raised on class: lte.X2TransportLayerAccess	Severity: indeterminate Specific problem: X2 LINK RESET DUE ON-LINE B-X2-INTERFACE CLASS PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates X2 link has reset when operator updates the value of B-X2-interface Class parameter on-line.		
Remedial action: No action is required.		

Table 29-2003 IK4905045

Alarm	Attributes	Applicable major release
Name: IK4905045 (3861) Type: communicationsAlarm Package: lte.IK4905045 Raised on class: lte.MmeTransportLayerAccess	Severity: indeterminate Specific problem: S1 LINK RESET DUE ON-LINE B-S1-INTERFACE CLASS PARAMETER UPDATE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates S1 link has reset when operator updates the value of B-S1-interface Class parameter on-line.		
Remedial action: No action is required.		

Table 29-2004 IK4905046

Alarm	Attributes	Applicable major release
Name: IK4905046 (3862) Type: equipmentAlarm Package: lte.IK4905046 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL OUTAGE START Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the cell has stopped to provide telecom services.		
Remedial action: No action is required.		

Table 29-2005 IK4905047

Alarm	Attributes	Applicable major release
Name: IK4905047 (3863) Type: equipmentAlarm Package: lte.IK4905047 Raised on class: lte.Cell	Severity: indeterminate Specific problem: CELL OUTAGE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the cell has started to provide telecom services.		
Remedial action: No action is required.		

Table 29-2006 IK4905048

Alarm	Attributes	Applicable major release
Name: IK4905048 (3864) Type: processingErrorAlarm Package: lte.IK4905048 Raised on class: lte.Cell	Severity: indeterminate Specific problem: OAM CELL EVENT 6 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: Provisioned for late churn-in. This event is for future use.		
Remedial action: No action is required.		

Table 29-2007 IK4905049

Alarm	Attributes	Applicable major release
Name: IK4905049 (3865) Type: processingErrorAlarm Package: lte.IK4905049 Raised on class: lte.Cell	Severity: indeterminate Specific problem: OAM CELL EVENT 7 Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-2007 IK4905049 (continued)

Alarm	Attributes	Applicable major release
Description: Provisioned for late churn-in. This event is for future use.		
Remedial action: No action is required.		

Table 29-2008 IK4905050

Alarm	Attributes	Applicable major release
Name: IK4905050 (3866) Type: equipmentAlarm Package: lte.IK4905050 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: MODULE WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a modem warm reset of the physical cell resource.		
Remedial action: No action is required.		

Table 29-2009 IK4905051

Alarm	Attributes	Applicable major release
Name: IK4905051 (3867) Type: equipmentAlarm Package: lte.IK4905051 Raised on class: lte.BBCardSpecifics	Severity: indeterminate Specific problem: LRA WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a local recovery action of the modem physical cell resource.		
Remedial action: No action is required.		

Table 29-2010 IK4905053

Alarm	Attributes	Applicable major release
Name: IK4905053 (3869) Type: processingErrorAlarm Package: lte.IK4905053 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: CMS INIT END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that operator enrollment scenario ended.		
Remedial action: No action is required.		

Table 29-2011 IK4905054

Alarm	Attributes	Applicable major release
Name: IK4905054 (3870) Type: processingErrorAlarm Package: lte.IK4905054 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: KEY UPDATE START Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the key updated started.		
Remedial action: No action is required.		

Table 29-2012 IK4905055

Alarm	Attributes	Applicable major release
Name: IK4905055 (3871) Type: processingErrorAlarm Package: lte.IK4905055 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: KEY UPDATE END Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the key updated ended.		
Remedial action: No action is required.		

Table 29-2013 IK4905061

Alarm	Attributes	Applicable major release
Name: IK4905061 (4156) Type: equipmentAlarm Package: lte.IK4905061 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the controller board is reset to restore the configuration data.		
Remedial action: No action is required.		

Table 29-2014 IK4905062

Alarm	Attributes	Applicable major release
Name: IK4905062 (4157) Type: equipmentAlarm Package: lte.IK4905062 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: CONTROLLER OAM RESET AFTER RESTORE WITH EMPTY DATABASE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L

Table 29-2014 IK4905062 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates an OAM auto-reset with an empty database as the database was not restored properly.		
Remedial action: No action is required.		

Table 29-2015 IK4905063

Alarm	Attributes	Applicable major release
Name: IK4905063 (4158) Type: communicationsAlarm Package: lte.IK4905063 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: DATABASE RECONFIGURATION RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that a reset was performed due to a database reconfiguration.		
Remedial action: No action is required.		

Table 29-2016 IK4905064

Alarm	Attributes	Applicable major release
Name: IK4905064 (4159) Type: equipmentAlarm Package: lte.IK4905064 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-2017 IK4905065

Alarm	Attributes	Applicable major release
Name: IK4905065 (4160) Type: equipmentAlarm Package: lte.IK4905065 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: LRA WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a local recovery action of the modem physical cell resource.		
Remedial action: No action is required.		

Table 29-2018 IK4905066

Alarm	Attributes	Applicable major release
Name: IK4905066 (4161) Type: equipmentAlarm Package: lte.IK4905066 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the main RFME antenna position coordinates have changed. The GPS antenna of the eNodeB has been moved or the mainAntennaPositionDeltaX/Y/Z values have been reconfigured.		
Remedial action: No action is required.		

Table 29-2019 IK4905067

Alarm	Attributes	Applicable major release
Name: IK4905067 (4162) Type: equipmentAlarm Package: lte.IK4905067 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MAIN ANTENNA POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the main RFME antenna position coordinates might not be correct.		
Remedial action: No action is required.		

Table 29-2020 IK4905068

Alarm	Attributes	Applicable major release
Name: IK4905068 (4163) Type: equipmentAlarm Package: lte.IK4905068 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MODULE RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2021 IK4905069

Alarm	Attributes	Applicable major release
Name: IK4905069 (4164) Type: equipmentAlarm Package: lte.IK4905069 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: MODULE WARM RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates a modem warm reset of the physical cell resource.		

Table 29-2021 IK4905069 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-2022 IK4905070

Alarm	Attributes	Applicable major release
Name: IK4905070 (4165) Type: equipmentAlarm Package: lte.IK4905070 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET CONTROLLER OAM ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2023 IK4905071

Alarm	Attributes	Applicable major release
Name: IK4905071 (4166) Type: equipmentAlarm Package: lte.IK4905071 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET OAM ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2024 IK4905072

Alarm	Attributes	Applicable major release
Name: IK4905072 (4167) Type: equipmentAlarm Package: lte.IK4905072 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: RESET ON OPERATOR REQUEST Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset command by the operator.		
Remedial action: No action is required.		

Table 29-2025 IK4905073

Alarm	Attributes	Applicable major release
Name: IK4905073 (4168) Type: equipmentAlarm Package: lte.IK4905073 Raised on class: lte.RFME	Severity: indeterminate Specific problem: LRA RESET Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates the reset due to a local recovery action.		
Remedial action: No action is required.		

Table 29-2026 IK4905083

Alarm	Attributes	Applicable major release
Name: IK4905083 (4789) Type: processingErrorAlarm Package: lte.IK4905083 Raised on class: lte.Cell	Severity: indeterminate Specific problem: AUTOMATED HANDOVER PARAMETER ADJUSTMENT COMPLETED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the SON process that automatically adjusts intra-frequency handover parameters has no further adjustments to make.		
Remedial action: No action is required.		

Table 29-2027 IK4905086

Alarm	Attributes	Applicable major release
Name: IK4905086 (4790) Type: equipmentAlarm Package: lte.IK4905086 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BBU POSITION CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BBU position coordinates have changed.		
Remedial action: No action is required.		

Table 29-2028 IK4905087

Alarm	Attributes	Applicable major release
Name: IK4905087 (4791) Type: equipmentAlarm Package: lte.IK4905087 Raised on class: lte.MODULE	Severity: indeterminate Specific problem: BBU POSITION ERROR Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L
Description: This event indicates that the BBU position coordinates might not be correct.		

Table 29-2028 IK4905087 (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action is required.		

Table 29-2029 IK4906001

Alarm	Attributes	Applicable major release
Name: IK4906001 (2831) Type: securityServiceOrMechanismViolation Package: lte.IK4906001 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: THREE UNSUCCESSFUL LOGIN ATTEMPTS Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the user failed to log into the eNodeB through SSH or CLI for three times in a span of 10 minutes.		
Remedial action: No action is required.		

Table 29-2030 IK4906002

Alarm	Attributes	Applicable major release
Name: IK4906002 (2832) Type: securityServiceOrMechanismViolation Package: lte.IK4906002 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SUCCESSFUL LOGIN Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the user successfully logged into the eNodeB through SSH or CLI.		
Remedial action: No action is required.		

Table 29-2031 IK4906003

Alarm	Attributes	Applicable major release
Name: IK4906003 (2833) Type: securityServiceOrMechanismViolation Package: lte.IK4906003 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: UNSUCCESSFUL LOGIN ATTEMPT Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the user failed to log into the eNodeB through SSH or CLI.		
Remedial action: No action is required.		

Table 29-2032 IK4906004

Alarm	Attributes	Applicable major release
Name: IK4906004 (2834) Type: securityServiceOrMechanismViolation Package: lte.IK4906004 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SUCCESSFUL ROLE CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that the user successfully changed roles on the eNodeB.		
Remedial action: No action is required.		

Table 29-2033 IK4906005

Alarm	Attributes	Applicable major release
Name: IK4906005 (2835) Type: securityServiceOrMechanismViolation Package: lte.IK4906005 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: UNSUCCESSFUL ROLE CHANGE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates the failure to change the user role on the eNodeB.		
Remedial action: No action is required.		

Table 29-2034 IK4906006

Alarm	Attributes	Applicable major release
Name: IK4906006 (2836) Type: physicalViolation Package: lte.IK4906006 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ETHERNET CABLE CONNECTED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that an Ethernet cable is connected to a port on the eNodeB.		
Remedial action: No action is required.		

Table 29-2035 IK4906007

Alarm	Attributes	Applicable major release
Name: IK4906007 (2837) Type: physicalViolation Package: lte.IK4906007 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: ETHERNET CABLE DISCONNECTED Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-2035 IK4906007 (continued)

Alarm	Attributes	Applicable major release
Description: This event indicates that an Ethernet cable is disconnected from a port on the eNodeB.		
Remedial action: No action is required.		

Table 29-2036 IK4906008

Alarm	Attributes	Applicable major release
Name: IK4906008 (2838) Type: integrityViolation Package: lte.IK4906008 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: SECURITY LOG ROLLED OVER Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates that a security log is rolled over.		
Remedial action: No action is required.		

Table 29-2037 IK4906010

Alarm	Attributes	Applicable major release
Name: IK4906010 (3302) Type: integrityViolation Package: lte.IK4906010 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: AUTHORIZATION LOG READ FAILURE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This event indicates a failure to read the SSH authorization log. The eNodeB is unable to log login attempts.		
Remedial action: No action is required.		

Table 29-2038 IK4906013

Alarm	Attributes	Applicable major release
Name: IK4906013 (8964) Type: securityServiceOrMechanismViolation Package: lte.IK4906013 Raised on class: lte.ENBEquipment	Severity: indeterminate Specific problem: DNS SERVICE UNAVAILABLE Implicitly cleared: true Default probable cause: unknown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm indicates that No DNS server at all is available for resolving a symbolic address to a numeric IP address		
Remedial action: No action is required.		

Table 29-2039 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 29-2040 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 29-2041 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		

Table 29-2041 LicensedLimitExceeded (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 29-2042 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 29-2043 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 29-2044 LTECellAdminDown

Alarm	Attributes	Applicable major release
Name: LTECellAdminDown (1471) Type: equipmentAlarm Package: lte.LTECellAdminDown Raised on class: lte.Cell	Severity: warning Specific problem: LTE Cell LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an LTE Cell Administrative State is down.		
Raising condition: (('administrativeState' NOT EQUAL 'Unlocked'))		
Clearing condition: (('administrativeState' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-2045 LTECellDegraded

Alarm	Attributes	Applicable major release
Name: LTECellDegraded (9559) Type: equipmentAlarm Package: lte.LTECellDegraded Raised on class: lte.Cell	Severity: major Specific problem: LTE Cell DEGRADED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an LTE Cell is not fully available.		
Raising condition: ('availabilityStatus'anyBit'Degraded')		
Clearing condition: NOT (('availabilityStatus'anyBit'Degraded'))		
Remedial action: The Cell is not fully available. AvailabilityStatus value and Additional attributes may indicate the nature and cause of the issue.		

Table 29-2046 LTECellDown

Alarm	Attributes	Applicable major release
Name: LTECellDown (1472) Type: equipmentAlarm Package: lte.LTECellDown Raised on class: lte.Cell	Severity: critical Specific problem: LTE Cell DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an LTE Cell is operationally down and availability status is failed or dependency.		
Raising condition: (('operationalState' EQUAL 'Disabled') AND ('administrativeState' EQUAL 'Unlocked') AND (('availabilityStatus'anyBit'Failed') OR ('availabilityStatus'anyBit'Dependency')))		
Clearing condition: (('administrativeState' EQUAL 'Locked') OR ('operationalState' EQUAL 'Enabled') OR NOT ((('availabilityStatus'anyBit'Failed') OR ('availabilityStatus'anyBit'Dependency'))))		
Remedial action: The Cell is inoperable. Additional attributes may indicate the nature and cause of the issue.		

Table 29-2047 M3MmeAccessAdminDown

Alarm	Attributes	Applicable major release
Name: M3MmeAccessAdminDown (4792) Type: equipmentAlarm Package: lte.M3MmeAccessAdminDown Raised on class: lte.M3MmeAccess	Severity: warning Specific problem: M3MmeAccess LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an M3MmeAccess Administrative State is down.		
Raising condition: (('Administrative State' NOT EQUAL 'Unlocked'))		
Clearing condition: (('Administrative State' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-2048 M3MmeAccessDegraded

Alarm	Attributes	Applicable major release
Name: M3MmeAccessDegraded (9560) Type: equipmentAlarm Package: lte.M3MmeAccessDegraded Raised on class: lte.M3MmeAccess	Severity: major Specific problem: M3MmeAccess DEGRADED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an M3MmeAccess is not fully available.		
Raising condition: ('Availability Status'anyBit'Degraded')		
Clearing condition: NOT (('Availability Status'anyBit'Degraded'))		
Remedial action: The Equipment is not fully available. AvailabilityStatus value and Additional attributes may indicate the nature and cause of the issue.		

Table 29-2049 M3MmeAccessDown

Alarm	Attributes	Applicable major release
Name: M3MmeAccessDown (4793) Type: equipmentAlarm Package: lte.M3MmeAccessDown Raised on class: lte.M3MmeAccess	Severity: critical Specific problem: M3MmeAccess DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an M3MmeAccess is operationally down.		
Raising condition: (('Operational State' EQUAL 'Disabled') AND ('Administrative State' EQUAL 'Unlocked') AND (('Availability Status'anyBit'Failed') OR ('Availability Status'anyBit'Dependency')))		
Clearing condition: (('Administrative State' EQUAL 'Locked') OR ('Operational State' EQUAL 'Enabled') OR NOT ((('Availability Status'anyBit'Failed') OR ('Availability Status'anyBit'Dependency'))))		

Table 29-2049 M3MmeAccessDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The Equipment is inoperable. Additional attributes may indicate the nature and cause of the issue.		

Table 29-2050 MmeAccessAdminDown

Alarm	Attributes	Applicable major release
Name: MmeAccessAdminDown (1523) Type: equipmentAlarm Package: lte.MmeAccessAdminDown Raised on class: lte.MmeAccess	Severity: warning Specific problem: MmeAccess LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an MME Access Administrative State is down.		
Raising condition: (('Administrative State' NOT EQUAL 'Unlocked'))		
Clearing condition: (('Administrative State' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-2051 MmeAccessDegraded

Alarm	Attributes	Applicable major release
Name: MmeAccessDegraded (9561) Type: equipmentAlarm Package: lte.MmeAccessDegraded Raised on class: lte.MmeAccess	Severity: major Specific problem: MmeAccess DEGRADED Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an MME Access is not fully available.		
Raising condition: ('Availability Status'anyBit'Degraded')		
Clearing condition: NOT (('Availability Status'anyBit'Degraded'))		
Remedial action: The Equipment is not fully available. AvailabilityStatus value and Additional attributes may indicate the nature and cause of the issue.		

Table 29-2052 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-2052 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 29-2053 MonitoredLinkStatusError

Alarm	Attributes	Applicable major release
Name: MonitoredLinkStatusError (4796) Type: processingErrorAlarm Package: lte.MonitoredLinkStatusError Raised on class: lte.ENBEquipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: corruptData	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the Network Element is reachable but the monitoring of link status fails. This alarm can be raised when several managers are managing a given Network Element which is not able to support multiple managers. The alarm can also be raised if the identifier of Network Element does not match the identifier in the Network Element managed in SAM. It is automatically cleared when the monitoring of the link status succeeds.		
Raising condition: ('OAM Link Status' EQUAL 'Down')		
Clearing condition: ('OAM Link Status' EQUAL 'Up')		
Remedial action: Network Element is reachable but the monitoring of link status fails		

Table 29-2054 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 29-2054 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 29-2055 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 29-2056 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 29-2057 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 29-2058 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 29-2059 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 29-2060 OutOfService

Alarm	Attributes	Applicable major release
Name: OutOfService (4385) Type: equipmentAlarm Package: netw.OutOfService Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an Equipment is detected as Out Of Service. For an ENB: the supervision link is down and all S1c Links between the ENB and its MMEs are down.		
Remedial action: The NE is Out of Service. Investigate on Site.		

Table 29-2061 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 29-2062 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		

Table 29-2062 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 29-2063 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 29-2064 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 29-2065 PMCMaxResultStringBlockSizeNotOptimum

Alarm	Attributes	Applicable major release
Name: PMCMaxResultStringBlockSizeNotOptimum (2922) Type: performanceOptimization Package: lte.PMCMaxResultStringBlockSizeNotOptimum Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongValue	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the PM maximum block size that will be transferred in one SNMP request is set to a value less than an optimum value of 6000 bytes. NOTE that the node's default value can be lower than 6000 bytes.		
Raising condition: ('pmcMaxResultStringBlockSize' < '6000')		
Clearing condition: ('pmcMaxResultStringBlockSize' >=" '6000')"		
Remedial action: Set blocksize to the recommended value.		

Table 29-2066 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 29-2067 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		

Table 29-2067 PrimaryImageBootFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 29-2068 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 29-2069 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 29-2070 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 29-2071 RncAccessAdminDown

Alarm	Attributes	Applicable major release
Name: RncAccessAdminDown (4797) Type: equipmentAlarm Package: lte.RncAccessAdminDown Raised on class: lte.RncAccess	Severity: warning Specific problem: Rnc Access DOWN Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when a RNC Access Administrative State is down.		
Raising condition: (('administrativeState' NOT EQUAL 'Unlocked'))		
Clearing condition: (('administrativeState' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

Table 29-2072 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 29-2073 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 29-2074 SelfOrganizingNetworkMisalignment

Alarm	Attributes	Applicable major release
Name: SelfOrganizingNetworkMisalignment (9562) Type: configurationAlarm Package: lte.SelfOrganizingNetworkMisalignment Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SONEventNotProcessed	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: SAM raises this alarm against the Network Element when SAM is temporally not able to proceed some SON Network Element configuration changes. When this alarm is raised, SAM tries periodically to resynchronize the entire Network Element configuration to solve any potential misalignment between the running Network Element configuration and the Network Element configuration in SAM. SAM automatically clears the alarm on successful full resynchronization.		
Remedial action: Informational only - self-correcting condition.		

Table 29-2075 SoftwareUpgradeDownloadFailed

Alarm	Attributes	Applicable major release
Name: SoftwareUpgradeDownloadFailed (3695) Type: communicationsAlarm Package: lte.SoftwareUpgradeDownloadFailed Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the transfer of software scheduled by a Self Config policy fails due to communication problem (communication timeout, cable disconnected). It is automatically cleared before starting a new upgrade scheduled by a Self Config policy.		
Remedial action: Check what happened during the File Transfer. Possible issues: Loss of NE Connectivity, FTP daemon down, FTP credential issues		

Table 29-2076 SoftwareUpgradeOperationNotAttempted

Alarm	Attributes	Applicable major release
Name: SoftwareUpgradeOperationNotAttempted (1963) Type: communicationsAlarm Package: lte.SoftwareUpgradeOperationNotAttempted Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bsCommunicationOffline	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the BS Communication State goes 'offline'. While BS communication state is 'offline' none of the Software Upgrade Operations can be attempted		
Clearing condition: (('bsCommunicationState' EQUAL 'omcManaged'))		
Remedial action: Release NEM sessions		

Table 29-2077 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 29-2078 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 29-2079 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 29-2080 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 29-2081 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • LR15.1.L • LR16.1.L • LR16.2.L

Table 29-2081 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 29-2082 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 29-2083 UDPPortAssignmentProblem

Alarm	Attributes	Applicable major release
Name: UDPPortAssignmentProblem (8026) Type: processingErrorAlarm Package: lte.UDPPortAssignmentProblem Raised on class: lte.CallTraceSessionManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when a NE's TCE UDP port cannot be updated.		
Remedial action: Ensure the NE is managed, reachable and that no configuration operation is in progress on that NE and relaunch the operation.		

Table 29-2084 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 29-2085 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 29-2086 UpgradeApplicationLockNotObtained

Alarm	Attributes	Applicable major release
Name: UpgradeApplicationLockNotObtained (1964) Type: integrityViolation Package: lte.UpgradeApplicationLockNotObtained Raised on class: lte.ENBEquipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnableToAcquireLock	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: This alarm is raised when the Software Upgrade Application is unable to acquire lock to start the operation. Retry the Software Upgrade Operation once the lock is released by the other application.		
Remedial action: Retry the Software Management Operation once the lock is released by the other application.		

Table 29-2087 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 29-2088 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 29-2089 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 29-2090 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 29-2091 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 29-2092 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 29-2093 X2AccessAdminDown

Alarm	Attributes	Applicable major release
Name: X2AccessAdminDown (1906) Type: equipmentAlarm Package: lte.X2AccessAdminDown Raised on class: lte.X2Access	Severity: warning Specific problem: X2 Access LOCKED BY OPERATOR Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • LR15.1.L • LR16.1.L • LR16.2.L
Description: The alarm is raised when an X2 Access Administrative State is down.		
Raising condition: (('Administrative State' NOT EQUAL 'Unlocked'))		
Clearing condition: (('Administrative State' EQUAL 'Unlocked'))		
Remedial action: Informational - no corrective action required.		

30 Cloud Mobility Manager

30.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 30-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 17.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 30-2 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 17.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 30-3 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 17.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 30-4 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 17.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 30-5 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 30-5 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 30-6 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 30-7 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 17.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 30-8 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 17.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 30-9 CmmCinderVolumeContentUnexpected

Alarm	Attributes	Applicable major release
Name: CmmCinderVolumeContentUnexpected (11810) Type: equipmentAlarm Package: ltecmm.CmmCinderVolumeContentUnexpected Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: userAction	Release: • 17.0.0
Description: Cinder volume folder structure is wrong		
Remedial action: Ensure that correct volume is attached. Detach wrong volume.		

Table 30-10 CmmCinderVolumeRemoved

Alarm	Attributes	Applicable major release
Name: CmmCinderVolumeRemoved (11811) Type: equipmentAlarm Package: ltecmm.CmmCinderVolumeRemoved Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: userAction	Release: • 17.0.0
Description: UDEV device manager notices that volume is disappeared.		
Remedial action: If volume is not detached by user then check Cinder volume by means of cinder and nova cli commands.		

Table 30-11 CmmLowMemoryResourceDbs

Alarm	Attributes	Applicable major release
Name: CmmLowMemoryResourceDbs (11821) Type: equipmentAlarm Package: ltecmm.CmmLowMemoryResourceDbs Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: serviceError	Release: • 17.0.0
Description: memory consumption on DBS reaches 75% (minor)memory consumption on DBS reaches 80% (major). VoltDB cluster switches to read-only mode.		
Remedial action: This alarm can only be cancelled via O&M interfaces.		

Table 30-12 CmmLSS_adnsExtendedTTLcaching

Alarm	Attributes	Applicable major release
Name: CmmLSS_adnsExtendedTTLcaching (11328) Type: equipmentAlarm Package: ltecmm.CmmLSS_ adnsExtendedTTLcaching Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates that extended TTL caching is being used by the enhanced DNS client on the NGSS / SIP Device Server (DS) cards.		
Remedial action: Nothing can be done specific to the NGSS / SIP DS card itself. DNS server connectivity paths and provisioning must be checked and verified to ensure proper response linkage between intra-LSS and extra-LSS DNS entities.Intra-LSS DNS connectivity should be first verified through procedural verification followed by Extra-LSS to network-level DNS server connectivity confirmation. Check the data at the DNS server to ensure that valid data is available.After 15 seconds where extended cache is not used this alarm alarm will clear itself automatically. If none of the steps above succeed in clearing the alarm, contact Customer Support.		

Table 30-13 CmmLSS_adnsQueryFailureCaching

Alarm	Attributes	Applicable major release
Name: CmmLSS_adnsQueryFailureCaching (11329) Type: equipmentAlarm Package: ltecmm.CmmLSS_ adnsQueryFailureCaching Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates that a failure response to a DNS query is received (either a failure response code was received from the DNS server, or no response was received from the DNS server) and no cache is available at the enhanced DNS client on the NGSS / SIP Device Server (DS) cards.		
Remedial action: Nothing can be done specific to the NGSS / SIP DS card itself. DNS server connectivity paths and provisioning must be checked and verified to ensure proper response linkage between intra-LSS and extra-LSS DNS entities.Intra-LSS DNS connectivity should be first verified through procedural verification followed by Extra-LSS to network-level DNS server connectivity confirmation. Check the data at the DNS server to ensure that valid data is available.After 15 seconds where no DNS queries failed due to no cache being available this alarm will clear itself automatically. If none of the steps above succeed in clearing the alarm, contact Customer Support.		

Table 30-14 CmmLSS_adnsQueueCongestion

Alarm	Attributes	Applicable major release
Name: CmmLSS_adnsQueueCongestion (11330) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_adnsQueueCongestion Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemResourcesOverloaded	Release: • 17.0.0
Description: This alarm indicates that aDNS does not have the ability to communicate with the local DNS client (unbound or bind). This could be caused either by a network issue, or the local DNS client is not running.		
Remedial action: Nothing can be done specific to the NGSS / SIP DS card itself. DNS server connectivity paths and provisioning must be checked and verified to ensure proper response linkage between aDNS and the local DNS client.Ensure that the local DNS client (either unbound or bind) is reachable, running and correctly configured.		

Table 30-15 CmmLSS_cardConnectionLost

Alarm	Attributes	Applicable major release
Name: CmmLSS_cardConnectionLost (11331) Type: equipmentAlarm Package: ltecmm.CmmLSS_cardConnectionLost Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: REM detected a problem with its connectivity to a service member under its control, or a service member has missed a heartbeat to REM.		
Remedial action: Verify the status on the service using REMcli. It should be "Out of Service". If it is active, or standby hot, with its mate being active, or manually out-of-service (unlocked/disabled/idle) then the alarm condition is not valid.If communication to the service does not come back within several minutes (e.g. the cardConnectionLost alarm does not clear), it may be necessary to connect to the card's console-port to get the status of the service. Consult card specific documentation about the console commands to obtain the card service state.If you are not successful in connecting to the console, this could be due to either a networking problem, or a fault in the card. If the the card is inaccessible via console, it can be recovered via the reset button, or by powercycling. Continued trouble may mean the card is having some hardware difficulty; and Customer Support should be contacted to determine the next step(s).Try to ping the internal fixed service ip address of the serivce member from the host which is running the active REM process. If pinging the service member from the VM succeeds, then go to Step 4; else go to Step 5.Determine if REM has a connection to the service member via the use of the netstat command on the host which has the active REM process The following command will give a list of IP addresses that REM has connected to via well-known port 20000:netstat -a | grep 20000Look for an "Established" connection to the service's IP address in the output of the above command. If the service's IP address is not found in the output and this is the first time you have visited this step, then go to Step 6. If the service's IP address is not found in the output and this is the second time you have visited this step, then go to Step 7.Check the IP connections from the host that has the active REM service member to the switches and the routers. Check the connection to the card. If connection problems are found, they must be fixed. One can also verify that the appropriate service IP addresses have been plumbed and the appropriate service image has been downloaded to the card.Try switching over the REM process.Restart/reload the service.		

Table 30-16 CmmLSS_cardStateChange

Alarm	Attributes	Applicable major release
Name: CmmLSS_cardStateChange (11332) Type: processingErrorAlarm Package: ltecmm.CmmLSS_cardStateChange Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: This alarm indicates that the state of a service or service member has changed. States are assigned to the two individual service members, as well as the service itself. The state change can be the result of a maintenance action or of a fault.		
Remedial action: No actions required.		

Table 30-17 CmmLSS_cmasFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_cmasFailure (11333) Type: processingErrorAlarm Package: ltecmm.CmmLSS_cmasFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: This alarm indicates that there is software failure in s1mme or sbc modules, related to CMAS.		
Remedial action: Contact Customer Support.		

Table 30-18 CmmLSS_cmasReceiveFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_cmasReceiveFailure (11334) Type: equipmentAlarm Package: ltecmm.CmmLSS_cmasReceiveFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates that MME failed to receive an acknowledgement to a CMAS message.		
Remedial action: Verify that the S1mme links are up.Alarm can only be cleared manually using CLI.If condition persists, contact Customer Support.		

Table 30-19 CmmLSS_cmasSendFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_cmasSendFailure (11335) Type: equipmentAlarm Package: ltecmm.CmmLSS_cmasSendFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates that there is a failure in sending a CMAS message over s1mme or sbc interfaces.		

Table 30-19 CmmLSS_cmasSendFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify that the S1mme and sbc links are up.Alarm can only be cleared manually via CLI.If condition persists, contact Customer Support.		

Table 30-20 CmmLSS_cpiAlrmCritical

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAlrmCritical (11336) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAlrmCritical Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAlrmCritical indicates the value of the VS.alrmCritical measurement monitored by the Critical Alarms Count CPI exceeded a threshold in the last 15 minute interval.This Performance Measurement (PM) counts the number of critical alarms issued by the reporting resource.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Using the Maintenance Interface, examine the set of critical alarms or any other alarms recently raised and address them.This alarm will clear automatically if the rate of critical alarm generation drops below the threshold.		

Table 30-21 CmmLSS_cpiAlrmMajor

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAlrmMajor (11337) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAlrmMajor Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAlrmMajor indicates the value of the VS.alrmMajor measurement monitored by the Major Alarms Count CPI exceeded a threshold in the last 15 minute interval.This Performance Measurement (PM) counts the number of major alarms issued by the reporting resource.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Using the Maintenance Interface, examine the set of major alarms or any other alarms recently raised and address them.This alarm will clear automatically if the rate of major alarm generation drops below the threshold.		

Table 30-22 CmmLSS_cpiAlrmMinor

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAlrmMinor (11338) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAlrmMinor Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-22 CmmLSS_cpiAlrmMinor (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiAlrmMinor indicates the value of the VS.alrmMinor measurement monitored by the Minor Alarms Count CPI exceeded a threshold in the last 15 minute interval.This Performance Measurement (PM) counts the number of minor alarms issued by the reporting resource.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Using the Maintenance Interface, examine the set of minor alarms or any other alarms recently raised and address them.This alarm will clear automatically if the rate of minor alarm generation drops below the threshold.		

Table 30-23 CmmLSS_cpiAsrtEsc

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAsrtEsc (11339) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAsrtEsc Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAsrtEsc indicates the value of the VS.asrtESC measurement monitored by the Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.In software, defensive checks are placed to ensure expected inputs or boundary conditions within routines are met. If such a check fails, an assert report is logged containing information for the code author to debug the problem. The assert messages themselves are not of much value to the operator.When the problem is serious enough, such as being associated with a critical resource, an assert that can result in escalation is used. Such asserts are tied to a leaky bucket mechanism that measures the rate of these events. If the specified thresholds are reached, a task restart is attempted. If that level of escalation continues to fail, then a process initialization is done which leads to a switch-over of the service. Immediate escalation is possible.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: This alarm will clear automatically if the rate of escalating assert generation drops below the threshold. An automatic escalation would result in a switch over and should also drop the rate of assert generation.Determine if any other alarms have been recently raised on the resource reported and address them.Examine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.If a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the PM counts indicates degradation of service and a switch over has not occurred, switch the service to its redundant mate.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.In all cases, contact customer support regarding this alarm.		

Table 30-24 CmmLSS_cpiAsrtNonEscCritical

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAsrtNonEscCritical (11340) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAsrtNonEscCritical Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-24 CmmLSS_cpiAsrtNonEscCritical (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiAsrtNonEscCritical indicates the value of the VS.asrtNonESCCritical measurement monitored by the Critical Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.In software, defensive checks are placed to ensure expected inputs or boundary conditions within routines are met. If such a check fails, an assert report is logged containing information for the code author to debug the problem. The assert messages themselves are not of much value to the operator. Most of the time asserts are isolated events; however, they can begin to accumulate in which case a more serious failure may be occurring for which this alarm is bringing attention to.Defensive checks are performed to prevent more serious outages if possible.Asserts, which do not invoke any automatic recovery through escalation, are tagged with levels of severity, in this case critical, to provide guidance to Customer Support on the seriousness of the problem.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.Determine if any other alarms have been recently raised on the resource reported and address them.Examine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.If a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the PM counts indicates degradation of service, switch the service to its redundant mate.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.In all cases, contact customer support regarding this alarm.		

Table 30-25 CmmLSS_cpiAsrtNonEscMajor

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAsrtNonEscMajor (11341) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAsrtNonEscMajor Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAsrtNonEscMajor indicates the value of the VS.asrtNonESCMajor measurement monitored by the Major Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.In software, defensive checks are placed to ensure expected inputs or boundary conditions within routines are met. If such a check fails, an assert report is logged containing information for the code author to debug the problem. The assert messages themselves are not of much value to the operator. Most of the time asserts are isolated events; however, they can begin to accumulate in which case a more serious failure may be occurring for which this alarm is bringing attention to.Defensive checks are performed to prevent more serious outages if possible.Asserts, which do not invoke any automatic recovery through escalation, are tagged with levels of severity, in this case major, to provide guidance to Customer Support on the seriousness of the problem.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.Determine if any other alarms have been recently raised on the resource reported and address them.Examine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.If a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the PM counts indicates degradation of service, switch the service to its redundant mate.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.In all cases, contact customer support regarding this alarm.		

Table 30-26 CmmLSS_cpiAsrtNonEscMinor

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAsrtNonEscMinor (11342) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAsrtNonEscMinor Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAsrtNonEscMinor indicates the value of the VS.asrtNonESCMinor measurement monitored by the Minor Non-Escalating Asserts CPI exceeded a threshold in the last 15 minute interval.In software, defensive checks are placed to ensure expected inputs or boundary conditions within routines are met. If such a check fails, an assert report is logged containing information for the code author to debug the problem. The assert messages themselves are not of much value to the operator. Most of the time asserts are isolated events; however, they can begin to accumulate in which case a more serious failure may be occurring for which this alarm is bringing attention to.Defensive checks are performed to prevent more serious outages if possible.Asserts, which do not invoke any automatic recovery through escalation, are tagged with levels of severity, in this case minor, to provide guidance to Customer Support on the seriousness of the problem.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: This alarm will clear automatically if the rate of non-escalating assert generation drops below the threshold.Determine if any other alarms have been recently raised on the resource reported and address them.Examine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.If a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the PM counts indicates degradation of service, switch the service to its redundant mate.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.In all cases, contact customer support regarding this alarm.		

Table 30-27 CmmLSS_cpiAttachFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAttachFailures (11343) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiAttachFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiAttachFailures, indicates the value of the VS.cpiAttachFailures measurement, monitored when failure Attach request CPI exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the UE Attach procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditionsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, HSS and SGW links are in-service/normal.If the links look normal, and the alarm persists, contact Customer Support.		

Table 30-28 CmmLSS_cpiAttachFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAttachFailuresSysRelated (11344) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiAttachFailuresSysRelated Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiAttachFailuresSysRelated, indicates meeting/exceeding a threshold of the rate of system-related failures for Attach procedures, which is calculated every 5 minutes, using the formula:VS.NbrAttachFailureSysRelated_ sum / VS.AttAttachRequestsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1, S6a and S11 links are in-service/normal.Verify that there are no overload alarms on the MMEContact Customer Support		

Table 30-29 CmmLSS_cpiAttachWithPGWreselection

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAttachWithPGWreselection (11345) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiAttachWithPGWreselection Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAttachWithPGWreselection indicates meeting a threshold of the rate of PGW reselection during Attach procedures CPI, which is calculated every 5 minutes using this formula:VS.AttachWithPGWreselection/VS. AttAttachRequestsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-30 CmmLSS_cpiAttachWithSGWreselection

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiAttachWithSGWreselection (11346) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiAttachWithSGWreselection Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiAttachWithSGWreselection indicates meeting a threshold of the rate of SGW reselection during Attach procedures CPI, which is calculated every 5 minutes using this formula:VS.AttachWithSGWreselection/VS. AttAttachRequestsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-30 CmmLSS_cpiAttachWithSGWreselection (continued)

Alarm	Attributes	Applicable major release
Remedial action: Contact Customer Support.		

Table 30-31 CmmLSS_cpiCreateDedicatedBearerFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiCreateDedicatedBearerFailures (11347) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiCreateDedicatedBearerFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiCreateDedicatedBearerFailures, indicates the value of VS.cpiCreateDedicatedBearerFailures measurement, monitored when failure on Create Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Create Dedicaed Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-32 CmmLSS_cpiDeactivateDedBearerFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiDeactivateDedBearerFailures (11348) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiDeactivateDedBearerFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiDeactivateDedBearerFailures, indicates the value of VS.cpiDeactivateDedBearerFailures measurement, monitored when failure on Deactivate Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Deactivate Dedicated Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-33 CmmLSS_cpiEIRfailuresS13

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiEIRfailuresS13 (11349) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiEIRfailuresS13 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-33 CmmLSS_cpiEIRfailuresS13 (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiEIRfailuresS13, indicates that the value of VS.LSS_cpiMafEIRfailuresS13 has exceeded a threshold in the last 5 minute interval. This counter monitors the percentage of unsuccessful EquipmentCheckRequest (ECR) to the number of ECRs attempted. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify the far end HSS (EIR) is functioning properly. Check fs.log for any ECR/ECA/S13 related errors to aid in determining the cause. Contact next level of support.		

Table 30-34 CmmLSS_cpiExtServiceReqFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiExtServiceReqFailuresSysRelated (11350) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiExtServiceReqFailuresSysRelated Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiExtServiceReqFailuresSysRelated indicates meeting a threshold of the Extended Service Request System Related Failure CPI, which is calculated every 5 minutes using this formula:100 * (VS. NbrFailedExtSvcRequestsSysRelated_sum / VS.AttExtServiceRequests)Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that S1, S6a, S11 and SGs links are Unlocked/EnabledVerify that there are no overload alarms on MMEContact Customer Support		

Table 30-35 CmmLSS_cpiExtServiceRequestFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiExtServiceRequestFailures (11351) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiExtServiceRequestFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiExtServiceRequestFailures indicates meeting a threshold of the Extended Service Request Failure CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS.NbrSuccessExtServiceRequests / VS. AttExtServiceRequests))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify MME provisioning data, especially PLMN, TAI-LAI-Mapping, LAI tablesVerify that S1, S6a, S11 and SGs links are Unlocked/EnabledVerify that there are no overload alarms on MMEContact Customer Support		

Table 30-36 CmmLSS_cpiFailuresOverSGs

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiFailuresOverSGs (11352) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiFailuresOverSGs Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiFailuresOverSGs, indicates meeting/exceeding a threshold of the rate of failure for handling messages from the SGs interface, which is calculated every 5 minutes, using the formula:VS.NbrFailedSGsSignalingProcedures / VS.AttSGsSignalingProceduresNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the SGs links are in-service/normalContact Customer Support		

Table 30-37 CmmLSS_cpiFileSysUsage

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiFileSysUsage (11353) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiFileSysUsage Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiFileSysUsage indicates the value of resource usage count VS.fileSysUsage monitored by the File System Usage CPI exceeded a threshold in the last 5-minute interval.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Remove outdated and obsolete files to free the file system space.Move the important data files to other disks to free the file system space.When CPI alarm LSS_cpiFileSysUsage is fired for CDR host, don't remove CDR record files (under /app1/data0/cdrdata) and PCMD record files (under /app1/data0/pcmddata). Furthermore, double check timestamp of CDR records files under /app1/data0/cdrdata/app2/charging/stream1/primary. If many files are older than two PULL/PUSH intervals, then there might be CDR records file transfer issue, which should be fixed firstly. For non-CDR record or non-PCMD record files, follow step 1 or step 2.		

Table 30-38 CmmLSS_cpiGTPcResponseTO_Gn

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiGTPcResponseTO_Gn (11354) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiGTPcResponseTO_Gn Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiGTPcResponseTO_Gn, indicates that the value of VS.cpiGTPcResponseTOGn has exceeded a threshold in the last 15 minute interval. This counter monitors the percentage of GTP Requests sent over a Gn interface for which no Response is received by the CMM. The Gn interface connects the CMM with one or more SGSNs. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-38 CmmLSS_cpiGTPcResponseTO_Gn (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check neighboring SGSNs for error conditions or ongoing problems. Verify network connectivity and proper configuration between CMM and SGSNs. If SGSNs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Gn interface have been reported. Contact next level of support.		

Table 30-39 CmmLSS_cpiGTPcResponseTO_S10

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiGTPcResponseTO_S10 (11355) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiGTPcResponseTO_S10 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiGTPcResponseTO_S10, indicates the value of VS.cpiGTPcResponseTO_S10 measurement, monitored when missing replies to S10(gtpc) request exceeded a threshold in the last 15 minute interval. This value computes the cpiage of Response messages that are not received over S10, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Check the network routers for any problems. Check to determine if any other MME elements are having problems.		

Table 30-40 CmmLSS_cpiGTPcResponseTO_S11

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiGTPcResponseTO_S11 (11356) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiGTPcResponseTO_S11 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiGTPcResponseTO_S11, indicates the value of VS.cpiGTPcResponseTO_S11 measurement, monitored when missing replies to S11(gtpc) request exceeded a threshold in the last 15 minute interval. This value computes the cpiage of Response messages that are not received over S11, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that S11 links are normal. If links are normal, and the alarm persists, contact Customer Support.		

Table 30-41 CmmLSS_cpiGTPcResponseTO_S3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiGTPcResponseTO_S3 (11357) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiGTPcResponseTO_S3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiGTPcResponseTO_S3, indicates meeting a threshold of GTP response failure rate in the last 5 minute interval. This failure rate monitors the percentage of GTP Requests sent over an S3 interface for which no Response is received by the MME. The S3 interface connects the MME with one or more SGSNs. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Check neighboring SGSNs for error conditions or ongoing problems. Verify network connectivity and proper configuration between MME and SGSNs. If SGSNs and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the S3 interface have been reported. Contact customer support.		

Table 30-42 CmmLSS_cpiGTPcResponseTO_Sv

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiGTPcResponseTO_Sv (11358) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiGTPcResponseTO_Sv Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiGTPcResponseTO_Sv indicates meeting a threshold of the GTPc Response Time out over Sv CPI (requests sent over an Sv interface for which no response is received), which is calculated every 5 minutes using this formula:VS.NbrTO_SvGtpc / VS.TotalReqSent_SvGtpcNotes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Check neighboring MSC(s) for error conditions or ongoing problems. Verify network connectivity and proper configuration between MME and MSC(s). If MSC(s) and network connectivity are verified, examine all the GTP failure counters to determine if one failure cause predominates, and check fs.log to determine if errors related to the Sv interface have been reported. Contact next level of support.		

Table 30-43 CmmLSS_cpiHOfailuresFromGERANoverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOfailuresFromGERANoverS3 (11361) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresFromGERANoverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-43 CmmLSS_cpiHOfailuresFromGERANoverS3 (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiHOfailuresFromGERANoverS3, indicates that the value of VS. cpiHOfailuresFromGERANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from GERAN to a E-UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-44 CmmLSS_cpiHOfailuresFromUTRANoverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOfailuresFromUTRANoverS3 (11362) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresFromUTRANoverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOfailuresFromUTRANoverS3, indicates that the value of VS. cpiHOfailuresFromUTRANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from UTRAN to a E-UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-45 CmmLSS_cpiHOfailuresRAUto2G3GnewSgwOverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiHOfailuresRAUto2G3GnewSgwOverS3 (11364) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresRAUto2G3GnewSgwOverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-45 CmmLSS_cpiHOfailuresRAUto2G3GnewSgwOverS3 (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GnewSgwOverS3, indicates that the value of VS. cpiHOfailuresRAUto2G3GnewSgwOverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted RAU-based handovers from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface with SGW Relocation. This is Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-46 CmmLSS_cpiHOfailuresRAUto2G3GOverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOfailuresRAUto2G3GOverS3 (11363) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresRAUto2G3GOverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GOverS3, indicates the failure rate of attempted Routing Area Update (RAU) procedures from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface has exceeded a threshold in the last 5 minute interval. Failures encountered during the entire duration of the RAU procedure are included. Therefore, failures encountered both prior to and after SGW change determination are included. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-47 CmmLSS_cpiHOfailuresRAUto2G3GsameSgwOverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiHOfailuresRAUto2G3GsameSgwOverS3 (11365) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresRAUto2G3GsameSgwOverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-47 CmmLSS_cpiHOfailuresRAUto2G3GsameSgwOverS3 (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiHOfailuresRAUto2G3GsameSgwOverS3, indicates that the value of VS. cpiHOfailuresRAUto2G3GsameSgwOverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN/GERAN SGSN using the S3 interface without SGW Relocation. This is Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-48 CmmLSS_cpiHOFailuresTo3G2GOverGn

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOFailuresTo3G2GOverGn (11359) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOFailuresTo3G2GOverGn Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOFailuresTo3G2GOverGn, indicates that the value of VS.cpiHOFailuresto3G2GOverGn has exceeded a threshold in the last 15 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN/GERAN SGSN using the Gn interface. This includes Routing Area Update procedures. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the Gn link status and MME service status.Check fs.log for error indications related to Gn interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-49 CmmLSS_cpiHOfailuresToGERANoverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOfailuresToGERANoverS3 (11366) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailuresToGERANoverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOfailuresToGERANoverS3, indicates that the value of VS.cpiHOfailuresToGERANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a GERAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-49 CmmLSS_cpiHOfailuresToGERANoverS3 (continued)

Alarm	Attributes	Applicable major release
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-50 CmmLSS_cpiHOFailuresToLTEOverGn

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOFailuresToLTEOverGn (11360) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOFailuresToLTEOverGn Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOFailuresToLTEOverGn, indicates that the value of (100 - (100 * (VS.NbrHOtoLTESuccessGn / VS.AttNbrHOtoLTEGn)) has has exceeded a threshold in the last 5 minute interval. This value monitors the percentage of failure rate of attempted handovers from GERAN/UTRAN to MME using the Gn interface. The calculated percentage is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the Gn link status and MME service status.Check fs.log for error indications related to Gn interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-51 CmmLSS_cpiHOfailurestoUTRANoverS3

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOfailurestoUTRANoverS3 (11367) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOfailurestoUTRANoverS3 Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOfailurestoUTRANoverS3, indicates that the value of VS.cpiHOfailuresToUTRANoverS3 has exceeded a threshold in the last 5 minute interval. This counter monitors the failure rate of attempted handovers from E-UTRAN to a UTRAN SGSN using the S3 interface. The failure rate is compared against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the SGSN, check the target UTRAN/GERAN network for errors related to inter-system mobility procedures.For failures attributed to the MME, check the S3 link status and MME service status.Check fs.log for error indications related to S3 interface procedures, contact next level of support if internal MME errors are indicated.		

Table 30-52 CmmLSS_cpiHOwMMErelocFailures_atSource

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOwMMErelocFailures_atSource (11368) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOwMMErelocFailures_atSource Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOwMMErelocFailures_atSource, indicates the value of VS.cpiHOwMMErelocFailures_ atSource measurement, monitored when failure on Handover request, with MME relocation, exceeded a threshold in the last 15 minute interval. This value computes the failure rate at the source MME for the Handover procedure with MME relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Look at all the failure counters for the Handover procedure with MME relocation (at the Source MME) in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 30-53 CmmLSS_cpiHOwMMErelocFailures_atTarget

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOwMMErelocFailures_atTarget (11369) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiHOwMMErelocFailures_atTarget Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOwMMErelocFailures_atTarget, indicates the value of VS.cpiHOwMMErelocFailures_atTarget measurement, monitored when failure on Handover request, with MME forward relocation, exceeded a threshold in the last 15 minute interval. This value computes the failure rate at the Target MME for the Handover procedure with MME relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Look at all the failure counters for the Handover procedure with MME relocation (at the Target MME) in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 30-54 CmmLSS_cpiHOwNoRelocFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOwNoRelocFailures (11370) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiHOwNoRelocFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-54 CmmLSS_cpiHOwNoRelocFailures (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiHOwNoRelocFailures, indicates the value of VS.cpiHOwNoRelocFailures measurement, monitored when failure on Handover Path Switch request, to same Serving Gateway, exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Handover procedure without MME relocation and without SGW relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-55 CmmLSS_cpiHOwSGWrelocFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHOwSGWrelocFailures (11371) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiHOwSGWrelocFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHOwSGWrelocFailures, indicates the value of VS.cpiHOwSGWrelocFailures measurement, monitored when failure on Handover Path Switch request, to a different Serving Gateway, exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Handover procedure without MME relocation and with SGW relocation, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Look at all the failure counters for the Handover procedure without MME relocation and with SGW relocation in the PMC XML files to determine if one failure cause predominates. If one is found, check User Documentation for any remedies specific to the found cause.		

Table 30-56 CmmLSS_cpiHSSauthFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHSSauthFailures (11372) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiHSSauthFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiHSSauthFailures, indicates the value of VS.cpiHSSauthFailures measurement, monitored when HSS failed Authentication requests exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Authentication procedure between the MME and the HSS, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditionsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Clearance options include:Ensure communication between the MME and HSS (ping)If the HSS (S6a) link looks normal, and alarm persists, contact Customer Support.		

Table 30-57 CmmLSS_cpiHSSreselection

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiHSSreselection (11373) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiHSSreselection Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiHSSreselection indicates meeting a threshold of the rate of HSS reselection during Authentication or Update Location procedures CPI, which is calculated every 5 minutes using this formula:VS.HssReselectionAtt/(VS.AttAuthRequestsHSS+VS.AttUpdateLocationRequest)Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-58 CmmLSS_cpiMBMSSessionStartM3FailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionStartM3FailureRate (11374) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionStartM3FailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionStartM3FailureRate indicates meeting a threshold of the MBMS Session Start M3 Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * ((VS.NbrSuccessMBMSsessionStartM3 + VS.AbortMBMSsessionStopM3) / VS.AttMBMSsessionStartM3))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.For failures attributed to the MME, check the M3 link status and MME service status.Check fs.log for error indications related to M3 interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-59 CmmLSS_cpiMBMSSessionStartSmFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionStartSmFailureRate (11375) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionStartSmFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionStartSmFailureRate indicates meeting a threshold of the MBMS Session Start Sm Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS.NbrSuccessMBMSsessionStartSm / VS.AttMBMSsessionStartSm))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-59 CmmLSS_cpiMBMSSessionStartSmFailureRate (continued)

Alarm	Attributes	Applicable major release
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.For failures attributed to the MME, check the Sm link status and MME service status.Check fs.log for error indications related to Sm interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-60 CmmLSS_cpiMBMSSessionStopM3FailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionStopM3FailureRate (11376) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionStopM3FailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionStopM3FailureRate indicates meeting a threshold of the MBMS Session Stop M3 Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * ((VS.NbrSuccessMBMSsessionStopM3 + VS.AbortMBMSsessionStopM3) / VS.AttMBMSsessionStopM3))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.For failures attributed to the MME, check the M3 link status and MME service status.Check fs.log for error indications related to M3 interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-61 CmmLSS_cpiMBMSSessionStopSmFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionStopSmFailureRate (11377) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionStopSmFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionStopSmFailureRate indicates meeting a threshold of the MBMS Session Stop Sm Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS.NbrSuccessMBMSsessionStopSm / VS.AttMBMSsessionStopSm))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.For failures attributed to the MME, check the Sm link status and MME service status.Check fs.log for error indications related to Sm interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-62 CmmLSS_cpiMBMSSessionUpdateM3FailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionUpdateM3FailureRate (11378) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionUpdateM3FailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionUpdateM3FailureRate indicates meeting a threshold of the MBMS Session Update M3 Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * ((VS. NbrSuccessMBMSsessionUpdateM3 + VS.AbortMBMSsessionStopM3) / VS.AttMBMSsessionUpdateM3))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the MCE, check the MCE/eNB and network connections for errors.For failures attributed to the MME, check the M3 link status and MME service status.Check fs.log for error indications related to M3 interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-63 CmmLSS_cpiMBMSSessionUpdateSmFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiMBMSSessionUpdateSmFailureRate (11379) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiMBMSSessionUpdateSmFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMBMSSessionUpdateSmFailureRate indicates meeting a threshold of the MBMS Session Update Sm Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS. NbrSuccessMBMSsessionUpdateSm / VS.AttMBMSsessionUpdateSm))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: For failures attributed to the MBMS-GW, check the MBMS-GW and network for errors.For failures attributed to the MME, check the Sm link status and MME service status.Check fs.log for error indications related to Sm interface procedures, contact Customer Support if internal MME errors are indicated.		

Table 30-64 CmmLSS_cpiMemAllocFail

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiMemAllocFail (11381) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiMemAllocFail Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-64 CmmLSS_cpiMemAllocFail (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiMemAllocFail, indicates the value of the VS.memAllocFail measurement monitored by the failed memory allocation attempts CPI exceeded a threshold in the last 15 minute interval.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Investigate the amount of load being handled by this service and take steps to reduce it if it is excessive. Otherwise contact Customer Support. If this alarm coincides with the introduction of a software update, contact Customer Support immediately.This alarm will clear automatically if the rate of memory allocation failures drops below the threshold.		

Table 30-65 CmmLSS_cpiMMEUEcapacity

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiMMEUEcapacity (11380) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiMMEUEcapacity Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiMMEUEcapacity, indicates meeting a threshold of a UE capacity utilization rate on a per board basis in the last 5 minutes. The utilization rate is calculated in every interval of 5 minutes by using this formula:(Number of maximum registered on a board / UE capacity of a single board) * 100%Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the subsequent intervals.		
Remedial action: Check how many board the CMM has and consider to install more board to increase the CMM capacity.		

Table 30-66 CmmLSS_cpiMobileTermLocRequestFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiMobileTermLocRequestFailures (11382) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiMobileTermLocRequestFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiMobileTermLocRequestFailures indicates meeting a threshold of the Mobile Termination Location Request Failure CPI, which is calculated every 5 minutes using this formula:1 - ((VS.NbrSuccessMobileTermLocRequests + VS.AbortMobileTermLocRequest_HO + VS.AbortMobileTermLocRequest_MMEreloc + VS.AbortMobileTermLocRequest_Other + VS.AbortMobileTermLocRequest_UEdetach) / VS.AttMobileTermLocRequests)Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1-MME and SLs links are in-service/normal.Refer to the Location Based Services failure counters to get a more specific failure reason.Contact Customer Support to determine the status of the SMLC that are involved in the LCS procedure.		

Table 30-67 CmmLSS_cpiNetwrkInducedLocRequestFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiNetwrkInducedLocRequestFailures (11383) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiNetwrkInducedLocRequestFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiNetwrkInducedLocRequestFailures indicates meeting a threshold of the Network Induced Location Request Failure CPI, which is calculated every 5 minutes using this formula:1 - ((VS.NbrSuccessNetwrkInducedLocRequests + VS.AbortNetwrkInducedLocRequest_HO + VS.AbortNetwrkInducedLocRequest_MMEreloc + VS.AbortNetwrkInducedLocRequest_ Other + VS.AbortNetwrkInducedLocRequest_UEdetach) / VS.AttNetwrkInducedLocRequests)Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1-MME and SLs links are in-service/normal.Refer to the Location Based Services failure counters to get a more specific failure reason.Contact Customer Support to determine the status of the SMLC that are involved in the LCS procedure.		

Table 30-68 CmmLSS_cpiNoPSHOFailuresOverSv

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiNoPSHOFailuresOverSv (11384) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiNoPSHOFailuresOverSv Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiNoPSHOFailuresOverSv indicates meeting a threshold of the Hand Down to UTRAN/GERAN via the Sv interface without PSHO Failure Rate CPI, which is calculated every 5 minutes using this formula:1 - ((VS. NbrSuccessCSHOSv + VS.NbrCSHOSvAbort_Other + VS.NbrCSHOSvAbort_Canceled) / VS.AttCSHOSv)Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Check counters and alarms related to the Sv interface. Verify network connectivity and proper configuration between the MME and MSC(s).Check the target UTRAN/GERAN network for configuration problems that could cause the handover preparation attempts to be rejected.Check the source E-UTRAN network and target UTRAN/GERAN network for handover failure conditions.Check fs.log for error indications related to Sv interface procedures. Contact next level of support if internal MME errors are indicated.		

Table 30-69 CmmLSS_cpiPDNconnWithPGWreselection

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiPDNconnWithPGWreselection (11385) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiPDNconnWithPGWreselection Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-69 CmmLSS_cpiPDNconnWithPGWreselection (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_cpiPDNconnWithPGWreselection indicates meeting a threshold of the rate of PGW reselection during PDN connectivity procedures CPI, which is calculated every 5 minutes using this formula:VS.PdnConnPgwReselection/VS.AttPDNConnReqNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-70 CmmLSS_cpiPSHOFailuresOverSv

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiPSHOFailuresOverSv (11386) Type: processingErrorAlarm Package: ltecmm.CmmLSS_cpiPSHOFailuresOverSv Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiPSHOFailuresOverSv indicates meeting a threshold of the Hand Down to UTRAN/GERAN via the Sv interface with PSHO Failure Rate CPI, which is calculated every 5 minutes using this formula:1 - ((VS.NbrSuccessPSHOSv + VS.NbrPSHOSvAbort_Other + VS.NbrPSHOSvAbort_Canceled) / VS.AttPSHOSv)Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Check counters and alarms related to the Sv interface. Verify network connectivity and proper configuration between the MME and MSC(s).Check the target UTRAN/GERAN network for configuration problems that could cause the handover preparation attempts to be rejected.Check the source E-UTRAN network and target UTRAN/GERAN network for handover failure conditions.Check fs.log for error indications related to Sv interface procedures. Contact next level of support if internal MME errors are indicated.		

Table 30-71 CmmLSS_cpiReinitServiceSelf

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiReinitServiceSelf (11387) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiReinitServiceSelf Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiReinitServiceSelf indicates the value of the VS.reinitServiceSelf measurement monitored by the Automatic Service Re-initialization CPI exceeded a threshold in the last 15 minute interval.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-71 CmmLSS_cpiReinitServiceSelf (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm will clear automatically if the rate of re-initializations drops below the threshold.Check that a switch over has successfully occurred.Determine if any other alarms have been recently raised on the resource reported and address them. As this is likely the result of recovery escalation, one or more of these alarms may also be raised: LSS_cpiAsrtEsc, LSS_cpiExceptionService, LSS_cpiRestartTaskIf a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service if that has not already occurred.If the situation persists after two or more switch-overs of the pair within the service, then attempt to duplex fail the service.Attempt to power down the card providing the service and then restore it. If the problem clears, this suggests faulty hardware.In all cases, contact customer support regarding this alarm.		

Table 30-72 CmmLSS_cpiRestartTask

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiRestartTask (11388) Type: processingErrorAlarm Package: ltecmm.CmmLSS_cpiRestartTask Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: The raised alarm LSS_cpiRestartTask indicates the value of the VS.restartTask measurement monitored by the Task Re-starts CPI exceeded a threshold in the last 15 minute interval.A restart is a fault recovery that is taken when a task (a.k.a. thread) within a resource (i.e., process in this case) performs an illegal operation (e.g., accessing an invalid address) or directly by the task when it enters an error leg that cannot recover the problem (the restart is directed by an assert call). The task's execution is halted at the point of the operation and resumed at its entry function.The intent is for one task restart to occur for a fault. However, if this fails, a leaky-bucket mechanism is also monitoring the rate of task restarts and an escalation to an initialization of the resource will occur if excessive. The initialization will also cause a switch over to the redundant mate.It is possible for more than one task to be undergoing restarts. These events are tied into this same PM count and the same leaky-bucket mechanism.Notes:The thresholds are configurable via CLI.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: This alarm will clear automatically if the rate of task restart occurrences drops below the threshold.Determine if any other alarms have been recently raised on the resource reported and address them.Examine the recent Performance (PM) counts on the resource reported; they may suggest more regarding this issue.If a provisioning or configuration change was executed just before the alarm was raised, consider that the change is causing the problem.If an Software Update (SU) or Patch is being soaked, then this could indicate a problem with the software delivered; immediately contact Customer Support.If the PM counts indicates degradation of service and a switch-over has not already occurred, switch the service to its redundant mate.If the situation persists after a switch-over, be sure that the prior active host of the service was removed from service and restored completely. Attempt another switch over to the original active host for the service.If the situation persists after two or more switch-overs of the pair within the service, then attempt to duplex fail the service.In all cases, contact customer support regarding this alarm.		

Table 30-73 CmmLSS_cpiS1MMEconnFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiS1MMEconnFailures (11389) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiS1MMEconnFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-73 CmmLSS_cpiS1MMEconnFailures (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiS1MMEconnFailures, indicates the value of VS.cpiS1MMEconnFailures measurement, monitored when failed S1MME Connect request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the eNB connection over S1-MME, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify PLMN or TAI provisioning data, via the CMM provisioning GUI. After validation of the data, if the problem persists, contact Customer Support.		

Table 30-74 CmmLSS_cpiS3TauFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiS3TauFailures (11390) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiS3TauFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiS3TauFailures, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link. This alarm is calculated every 5 minutes using the formula:(VS.TauAttS3 - VS.TauSuccS3) / VS.TauAttS3Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal.Verify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.Verify the operational status of the DNS server and that the DNS entries for the SGW are correct.Contact Customer Support to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 30-75 CmmLSS_cpiS3TauFailuresInterSgw

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiS3TauFailuresInterSgw (11391) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiS3TauFailuresInterSgw Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiS3TauFailuresInterSgw, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link that involves a change of serving SGW. This alarm is calculated every 5 minutes using the formula:(VS.TauInterSgwAttS3 - VS.TauInterSgwSuccS3) / VS.TauInterSgwAttS3Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal.Verify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.Verify the operational status of the DNS server and that the DNS entries for the SGW are correct.Contact Customer Support to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 30-76 CmmLSS_cpiS3TauFailuresIntraSGW

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiS3TauFailuresIntraSGW (11392) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiS3TauFailuresIntraSGW Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiS3TauFailuresIntraSGW, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures from an SGSN to the MME over an S3 link that do not involve a change of serving SGW. This alarm is calculated every 5 minutes using the formula:(VS.TauIntraSgwAttS3 - VS.TauIntraSgwSuccS3) / VS.TauIntraSgwAttS3Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, SGW, HSS, and SGSN S3 links are in-service/normal.Verify the operational status of the SGSN and that the SGSN is responding to messages over the S3 link.Verify the operational status of the DNS server and that the DNS entries for the SGW are correct.Contact Customer Support to determine the status of the serving eNB, the HSS and the SGW serving the eNB that is involved in the TAU procedure.		

Table 30-77 CmmLSS_cpiServiceReqFailuresSysRelated

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiServiceReqFailuresSysRelated (11393) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiServiceReqFailuresSysRelated Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiServiceReqFailuresSysRelated, indicates meeting/exceeding a threshold of the rate of system-related failures for UE Service Request procedures, which is calculated every 5 minutes, using the formula:VS. NbrServiceReqFailureSysRelated_sum / VS.AttServiceRequestsNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1, S6a and S11 links are in-service/normal.Verify that there are no overload alarms on the MMEContact Customer Support		

Table 30-78 CmmLSS_cpiServiceRequestFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiServiceRequestFailures (11394) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiServiceRequestFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-78 CmmLSS_cpiServiceRequestFailures (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiServiceRequestFailures, indicates the value of cpiServiceRequestFailures measurement, monitored when failure on Service request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the UE Service Request procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Ensure the S11 links to SGW are normal. If the links look normal, and alarm persists, contact Customer Support.		

Table 30-79 CmmLSS_cpiStopWarnMsgDeliveryS1MMEFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiStopWarnMsgDeliveryS1MMEFailureRate (11395) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiStopWarnMsgDeliveryS1MMEFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiStopWarnMsgDeliveryS1MMEFailureRate indicates meeting a threshold of the Stop Warning Message Delivery S1MME Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS. NbrSuccessStopWarnMsgDeliveryS1MME / VS.AttStopWarnMsgDeliveryS1MME))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1MME links are in-service/normal.Verify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.Verify the MME_TAI table contains the correct TAIs.Contact Customer Support to determine the status of the eNBs that are involved in the Stop Warning Message procedure.		

Table 30-80 CmmLSS_cpiStopWarnMsgDeliverySBcFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_ cpiStopWarnMsgDeliverySBcFailureRate (11396) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiStopWarnMsgDeliverySBcFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiStopWarnMsgDeliverySBcFailureRate indicates meeting a threshold of the Stop Warning Message Delivery SBc Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS. NbrSuccessStopWarnMsgDeliverySBc / VS.AttStopWarnMsgDeliverySBc))Notes:The thresholds are configurable within this contextAn alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the SBC links are in-service/normal.Verify that the S1MME links are in-service/normal.Verify the operational status of the CBC.Verify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.Verify the MME_TAI table contains the correct TAIs.Contact Customer Support to determine the status of the CBC and eNBs that are involved in the Stop Warning Message procedure.		

Table 30-81 CmmLSS_cpiTauFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiTauFailures (11397) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiTauFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiTauFailures, indicates the value of VS.cpiTauFailures measurement, monitored when failure on Tracking Area Update request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the TAU procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Contact Customer Support.		

Table 30-82 CmmLSS_cpiTauFailuresInterMme

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiTauFailuresInterMme (11398) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiTauFailuresInterMme Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiTauFailuresInterMme, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving MME relocation which is calculated every 5 minutes, using the formula:(VS.TauInterMmeAtt - VS.TauInterMmeSucc) / VS.TauInterMmeAttNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, and MME links are in-service/normal.Contact Customer Support to determine the status of the serving eNB and the MME groups serving the eNB that is involved in the TAU procedure		

Table 30-83 CmmLSS_cpiTauFailuresInterMmeInterSgw

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiTauFailuresInterMmeInterSgw (11399) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiTauFailuresInterMmeInterSgw Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiTauFailuresInterMmeInterSgw, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving MME relocation and SGW relocation which is calculated every 5 minutes, using the formula:(VS.TauInterMmeInterSgwAtt - VS.TauInterMmeInterSgwSucc) / VS.TauInterMmeInterSgwAttNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		

Table 30-83 CmmLSS_cpiTauFailuresInterMmeInterSgw (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify that the HSS, eNB, SGW, and MME links are in-service/normal.Verify UE subscription information in HSS.Contact Customer Support to determine the status of the serving eNB, MME groups, and SGW Pools serving the eNB that are involved in the TAU procedure.		

Table 30-84 CmmLSS_cpiTauFailuresInterSgw

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiTauFailuresInterSgw (11400) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiTauFailuresInterSgw Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiTauFailuresInterSgw, indicates meeting/exceeding a threshold of the rate of failure of Tracking Area Update procedures involving SGW relocation, which is calculated every 5 minutes, using the formula:(VS.TauInterSgwSucc - VS.TauInterSgwAtt) / VS.TauInterSgwAttNotes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the eNB, and SGW links are in-service/normal.Contact Customer Support to determine the status of the serving eNB and the SGW Pools serving the eNB that is involved in the TAU procedure		

Table 30-85 CmmLSS_cpiUEauthFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiUEauthFailures (11401) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiUEauthFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiUEauthFailures, indicates the value of VS.cpiUEauthFailures measurement, monitored when UE failed Authentication requests exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Authentication procedure between the MME and the UE and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The thresholds are configurable within this context.An alarm with the same severity is raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify HSS and UE authentication data, using ueadmin_cli.If the authentication data looks good, and the alarm persists, contact Customer Support.		

Table 30-86 CmmLSS_cpiUpdateBearerFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiUpdateBearerFailures (11402) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiUpdateBearerFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-86 CmmLSS_cpiUpdateBearerFailures (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm, LSS_cpiUpdateBearerFailures, indicates the value of cpiUpdateBearerFailures measurement, monitored when failure on Update Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Update Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Ensure S11 links are normal. If the links are normal, and the alarm persists, contact Customer Support.		

Table 30-87 CmmLSS_cpiUpdateDedicatedBearerFailures

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiUpdateDedicatedBearerFailures (11403) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiUpdateDedicatedBearerFailures Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm, LSS_cpiUpdateDedicatedBearerFailures, indicates the value of VS.cpiUpdateDedicatedBearerFailures measurement, monitored when failure on Update Dedicated Bearer request exceeded a threshold in the last 15 minute interval. This value computes the failure rate for the Update Dedicated Bearer procedure, and compares the calculation against provisioned thresholds for Minor, Major, and Critical alarm conditions.Notes:The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that S11 links are normal. If links are normal, and the alarm persists, contact Customer Support.		

Table 30-88 CmmLSS_cpiWarnMsgDeliveryS1MMEFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiWarnMsgDeliveryS1MMEFailureRate (11404) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_cpiWarnMsgDeliveryS1MMEFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiWarnMsgDeliveryS1MMEFailureRate indicates meeting a threshold of the Warning Message Delivery S1MME Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS.NbrSuccessWarnMsgDeliveryS1MME / VS.AttWarnMsgDeliveryS1MME))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the S1MME links are in-service/normal.Verify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.Verify the MME_TAI table contains the correct TAIs.Contact Customer Support to determine the status of the eNBs that are involved in the Write Replace Warning Message procedure.		

Table 30-89 CmmLSS_cpiWarnMsgDeliverySBcFailureRate

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpiWarnMsgDeliverySBcFailureRate (11405) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ cpiWarnMsgDeliverySBcFailureRate Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The raised alarm LSS_cpiWarnMsgDeliverySBcFailureRate indicates meeting a threshold of the Warning Message Delivery SBc Failure Rate CPI, which is calculated every 5 minutes using this formula:100 - (100 * (VS. NbrSuccessWarnMsgDeliverySBc / VS.AttWarnMsgDeliverySBc))Notes:The thresholds are configurable within this context.An alarm with the same severity will be raised only once for the same CPI and component.The alarm will be cleared if no threshold is met in one of the following intervals.		
Remedial action: Verify that the SBC links are in-service/normal.Verify that the S1MME links are in-service/normal.Verify the operational status of the CBC.Verify the operational status of the eNBs and that the eNBs are responding to messages over the S1MME link.Verify the MME_TAI table contains the correct TAIs.Contact Customer Support to determine the status of the CBC and eNBs that are involved in the Write Replace Warning Message procedure.		

Table 30-90 CmmLSS_cpuOverload

Alarm	Attributes	Applicable major release
Name: CmmLSS_cpuOverload (11406) Type: processingErrorAlarm Package: ltecmm.CmmLSS_cpuOverload Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpuCycleLimitExceeded	Release: • 17.0.0
Description: This alarm indicates that the CPU utilization on a service has exceeded the threshold. The overload could be caused by one or more of the following reasons: base overload, per-service quota restriction overload or thread level CPU overload. The 'Additional Info' field of the alarm report will list the contributing causes. When thread level CPU overload level changes, a corresponding profile report is also generated.		
Remedial action: Verify that no running debug or testing tool is running that uses a lot of CPU.If CPU utilization regularly exceeds thresholds, investigate how the call traffic load can be reduced:Reengineer so less traffic is directed to this office or card.If CPU utilization regularly exceeds thresholds, investigate how to re-engineer the system so less traffic is directed to this service. If the problem persists, please contact the customer support team for further investigation.		

Table 30-91 CmmLSS_dataMismatch

Alarm	Attributes	Applicable major release
Name: CmmLSS_dataMismatch (11407) Type: processingErrorAlarm Package: ltecmm.CmmLSS_dataMismatch Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomiz-ingError	Release: • 17.0.0

Table 30-91 CmmLSS_dataMismatch (continued)

Alarm	Attributes	Applicable major release
Description: A data mismatch has been detected, which indicates that there has been an error in provisioning. The additionalText field of the event provides the details of the data mismatch. Currently supported data mismatches are listed in the table below: IdentifierResourceExplanationMH_SH_PROVISIONINGCMM link(S1mme, S6a, S13, SGs)An interface profile has been associated with an SCTP profile that indicates either single-homed or multi-homed, but the network interface types (ni-types) associated with a network interface do not match that configuration. For example for SGs, the singled-homed ni-type is SGS, and the multi-homed ni-types are SGS_1 and SGS_2, so if the SCTP profile indicates single-homed, an SGs network interface must have an ni-type type of SGS, and if the SCTP profile indicates multi-homed, an SGs interface must have ni-types of SGS_1 and SGS_2. The additionalText field indicates the type of homing provisioned and the inconsistency found.MH_PROVISIONED_IPSLinkAn SCTP multi-homed link has been provisioned with remote adrresses that do not match the addresses that were learned from the remote end in the INIT-ACK message. There is either a provisioning mistake on the CMM, or on the remote end of the connection. The additionalText field of the event will indicate the provisioned (LCL) IP addresses and the remote (RMT) learned addresses which caused the descrepancy. The state of each IP address will be indicated after the IP address , e.g. 1.2.3.4(STATE), where STATE is one of; R - reachable, U - unreachable, C - unconfirmed.This alarm must be manually cleared after the provisioned data is corrected.		
Remedial action: The following table indicates the recovery procedure for the events referred to by their identifier in the previous table:IdentifierRecovery ProcedureMH_SH_PROVISIONINGCorrect the SCTP profile for this link type to indicate the correct homing type (SH or MH), or configure the correct ni-types for the link, so that they match the SCTP profile.MH_PROVISIONED_IPSCorrect the provisioning of the locally provisioned remote IPs to match the learned remote IPs, or change the provisioning on the remote end to match the locally provisioned remote IPs.		

Table 30-92 CmmLSS_degradedResource

Alarm	Attributes	Applicable major release
Name: CmmLSS_degradedResource (11408) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_degradedResource Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: performanceDegraded	Release: • 17.0.0
Description: A Critical Application Resource (CAR) has reached a degraded condition that indicates some aspect of the switch is not performing as expected. The affected service member is indicated in the alarm by the PoolType, PoolId, and PoolMemberId.		

Table 30-92 CmmLSS_degradedResource (continued)

Alarm	Attributes	Applicable major release
Remedial action: From the alarm, determine the service member that is degraded, as shown by the PoolType, PoolId, and PoolMemberId.The following table lists the resources that exist for each service type, and the associated alarm for each that has one. In most cases, when a resource is degraded, the associated alarm will be firing. The associated alarm documentation can be viewed by clicking the link in the appropriate table below. If the associated alarm is firing, refer to its documentation to resolve the problem. If the associated alarm is not firing, or no associated alarm is defined, contact Customer Support.Critical Application ResourceService typesCAR TypeAssociated Alarm: LSS_*ThresholdExplanationCommunication to CPPSIPDSBoolSingleinternalCommunicationFailureN/ARepresents the MME internal communication status on IPDS. This CAR is off normal when IPDS can not communicate with CPPS.Communication to IPDSCPPSBoolSingleinternalCommunicationFailureN/ ARepresents the MME internal communication status on CPPS. This CAR is off normal when CPPS can not communicate with IPDS.CPU overloadall disklessBoolSinglecpuOverloadN/ARepresents critical CPU overload. It is off normal when the service member is in critical CPU overload, which by default is 95%.CxnMgr connectionsCPPSBoolSinglesoftwareAllocatedResourceOverloadN/ ARepresents preallocated resource for Connection Manager software module on CPPS. Each CPPS has its own Connection Manager resource allocation. This CAR is off normal if the Connection Manager resource usage is above its critical overload threshold.File system usageCDRBoolSingldiskSpaceExhaustedN/ARepresents the usage of disk space on a CDR, which stores CDR records. If the disk space usage reaches Major threshold (default is 85%), the CAR is off normal. IMSIMapDBIPDSBoolSinglesoftwareAllocatedResourceOverloadN/ARepresents preallocated memory for IMSIMapDB software module on IPDS. This CAR is off normal if the IMSIMapDB resource usage is above its critical overload threshold.Internal MME communicationall MME disklessBoolSingleinternalCommunicationFailureN/ARepresents all of an MME diskless service member's internal links to other MME diskless service members. The CAR is off normal when all internal MME communications are down.Internal linksall disklessBoolGrouplogicalLinkDown1%Represents a diskless service member's internal links to other diskless service members. Each member represents a link between this diskless service member and another diskless service member, and the member number is the IP address of the other diskless service member. The member is off normal when the link is down.Memory overloadall disklessBoolSinglememoryOverloadN/ARepresents critical memory overload. It is off normal when the service member is in critical memory overload, which by default is 90%.PCMD FTP pushCDRBoolSingleftpDownN/ARepresents FTP transfer of PCMD data between CDR and northbound interface. The CAR is off normal when PCMD data transfer between CDR and northbound interface failed with FTP method.PCMD SSH pushCDRBoolSinglescpDownN/ARepresents SSH transfer of PCMD data between CDR and northbound interface. The CAR is off normal when PCMD data transfer between CDR and northbound interface failed with SSH method.Rcvr to PCMD logger connectionCDRBoolSinglecdrPCMDReceiverTcpDownN/ARepresents the PCMD logger connection with the local CDR receiver. The CAR is off normal when the connection is broken.S11 linksIPDSBoolGroupexternalLinkDown100% Represents S11 link status on MME. Each CAR member represents one S11 link. The member number is the link index. The CAR member is off normal if the link is down.S13 linksIPDSBoolGroupexternalLinkDown100%Represents S13 link status on MME. Each CAR member represents one S13 link. The member number is the link index. The CAR member is off normal if the link is down.S1mme linksIPDSTankSingleexternalLinkDown100%Represents the status of all S1mme links on MME. The CAR is off normal if all of the links are down.S6a linksIPDSBoolGroupexternalLinkDown100%Represents S6a link status on MME. Each CAR member represents one S6a link. The member number is the link index. The CAR member is off normal if the link is down.SCTP bufferSS7BoolSinglesctpBufferExhaustionN/ARepresents the SCTP sending buffer usage status. When SCTP sending buffer usage exceeds 60%, the CAR will report off normal. When the SCTP association is reset or the SCTP sending buffer usage comes down from above 60% to below 60%, the CAR will report normal.SCTP congestionSS7BoolSinglesctpCongestionN/ARepresents the SCTP association congestion status. The CAR will report off normal under following conditions: 1) the SCTP acknowledgement delay exceeded 3 seconds or 2) the data size to be sent exceeded the peer's congestion control window equal to or more than 10 times within 5 minutes. The CAR will report normal under following conditions: 1) there was no SCTP acknowledgement delay that exceeded 3 seconds in the last 5 minutes and 2) the data size to be sent exceeded the peer's congestion control window less than 10 times in last 5 minutes.SessDist bufferCPPSBoolSinglesoftwareAllocatedResourceOverloadN/ARepresents preallocated buffer for Session Distributor software module on CPPS. Each CPPS has its own Session Distributor buffer allocation. This CAR is off normal if the Session Distributor buffer usage is above its critical overload threshold.SMLCSS7BoolGroupN/A1%Represents the SMLC status. Each CAR member represents one SMLC. The member number is the controller index. The CAR members are registered only on the active SS7s. If the SMLC cannot come into the IN SERVICE state, then this CAR member will report off normal.		

Table 30-93 CmmLSS_deviceServerCxnLost

Alarm	Attributes	Applicable major release
Name: CmmLSS_deviceServerCxnLost (11409) Type: equipmentAlarm Package: ltecmm.CmmLSS_deviceServerCxnLost Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm is generated when the mate-to-mate connection is lost for some service instance pairs.		
Remedial action: The alarm clears automatically when the switch-over is completed.If the alarm is not the result of a manual action, then the alarm will automatically clear within a minute. Customer Technical Support should be contacted if the alarm does not clear automatically.If the alarm is the result of a manual action, such as taking a host out of service, then the alarm will clear when the host is manually placed back into service.		

Table 30-94 CmmLSS_diamLinkDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_diamLinkDown (11410) Type: equipmentAlarm Package: ltecmm.CmmLSS_diamLinkDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 17.0.0
Description: Indicates that individual, some or all of the Diameter (Agent) connections are down for Geographic Redundancy or Multiple Destinations strategy.		
Remedial action: Once the connection is lost, fault recovery software on diameter client side will periodically retry to establish the connection with the diameter server side.Need to check configuration of Diameter peers and make sure that Diameter server is listening successfully with right port.Contact Customer Support if the alarm is not cleared.		

Table 30-95 CmmLSS_diamMaxClientsExceeded

Alarm	Attributes	Applicable major release
Name: CmmLSS_diamMaxClientsExceeded (11411) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_diamMaxClientsExceeded Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemResourcesOverloaded	Release: • 17.0.0
Description: This alarm indicates that number of clients exceeds the max allowed number of clients on server side.		
Remedial action: Once too many clients connecting to the same Diameter server, need to check what maximum value is configured in the server.If the maximum value in server is right, new clients can only be handled by retrying later after the number of clients comes back to below the max number.Contact Customer Support if the alarm is not cleared after retrying number is already below the max number.		

Table 30-96 CmmLSS_dnsThreshold

Alarm	Attributes	Applicable major release
Name: CmmLSS_dnsThreshold (11412) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_dnsThreshold Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemResourcesOverloaded	Release: • 17.0.0
Description: This alarm indicates returned number of IP addresses in DNS query of diameter fully-qualified domain name (FQDN) exceeds its number threshold.		
Remedial action: Verify that destination FQDN is correctly provisioned on the GUIVerify that FQDN is correctly provisioned on the external DNS server(IP addresses count should be less than threshold value).		

Table 30-97 CmmLSS_ethernetError

Alarm	Attributes	Applicable major release
Name: CmmLSS_ethernetError (11413) Type: equipmentAlarm Package: ltecmm.CmmLSS_ethernetError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: One of the two Ethernet Links on a Service Host has failed.		
Remedial action: Regardless of the cause of the Ethernet Link alarm, integrity software running on the affected Service Host should automatically initiate a switch to redundant hardware to ensure that the effects of the failure are minimized. The following recovery actions may, in fact, be automatically initiated:Service Host switch, if multiple Ethernet Links are affectedEthernet Link switch, if a single Active Ethernet Link is affectedNone, if the hardware failure affects a Standby Ethernet LinkThe reason for the failure needs to be understood and corrected. It is possible that the Service Host Ethernet Port failed, the cabling that interconnects the Ethernet Port to the network is cut, the Routers and/or Ethernet Switches that make up theSoftSwitch Network failed. Each of these possible reasons needs to be investigated and discounted or corrected by maintenance personnel. Once corrected, the alarm will be cleared.		

Table 30-98 CmmLSS_ethernetLinkDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_ethernetLinkDown (11414) Type: equipmentAlarm Package: ltecmm.CmmLSS_ethernetLinkDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: The redundant Ethernet link has gone down on one of the diskless hosts. A link switchover may have occurred to move communication for that host to the remaining link, which is now simplex.		
Remedial action: Determine if any related alarms are also present. Correct those alarms first and see if this alarm clears as a result.If the above steps do not clear the alarm, contact Customer Support.		

Table 30-99 CmmLSS_ethernetLinkStateChange

Alarm	Attributes	Applicable major release
Name: CmmLSS_ethernetLinkStateChange (11812) Type: processingErrorAlarm Package: ltecmm.CmmLSS_ethernetLinkStateChange Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: One of the Ethernet Links on a Service Host has changed state.		
Remedial action: No actions required.		

Table 30-100 CmmLSS_excessiveExtCommFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_excessiveExtCommFailure (11813) Type: communicationsAlarm Package: ltecmm.CmmLSS_ excessiveExtCommFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: An excessive number of network elements of a given type (e.g. RNC) are having communication failure with the CMM. This is usually due to a network connectivity problem and not the individual external network element. Once this alarm is triggered the CMM will stop reporting alarms for the network element of the given type. Once the network problem is resolved and the alarm no longer excessive, this alarm will clear. This alarm is raised when at least 100 network elements of a given type having communication failure. This alarm clears when 95 or fewer are having communication failure.		
Remedial action: Determine that there are no errors within the IP network.If the network entity data is provisioned on CMM, verify the data is correct.Verify the network entity that CMM fails to communicate with is in service.		

Table 30-101 CmmLSS_excessiveExternalLinksDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_excessiveExternalLinksDown (11415) Type: communicationsAlarm Package: ltecmm.CmmLSS_ excessiveExternalLinksDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: An excessive number of links of a given type (e.g. s1mme, s11, etc.) are down. This is usually due to a network connectivity problem and not the individual links between the CMM and the external entity. Once this alarm is triggered the CMM will stop reporting alarms and status for links of the given type. Once the network problem is resolved and the number of links down is no longer excessive, this alarm will clear and the status of all links of the given type will be updated. This alarm is raised when at least 100 links of a given type are down. This alarm clears when 95 or fewer links are down.		
Remedial action: Determine that there are no errors within the IP network.If the network entity data is provisioned on MME, verify the data is correct.Verify the network entity that MME fails to communicate with is in service.		

Table 30-102 CmmLSS_externalCommFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_externalCommFailure (11814) Type: communicationsAlarm Package: ltecmm.CmmLSS_externalCommFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: Communication between CMM and another network entity can not be established. The additional text field indicates the specific entity involved.		
Remedial action: Verify the network entity that CMM fails to communicate with is in service.Determine that there are no errors within the IP network.If the network entity data is provisioned on CMM, verify the data is correct.If multiple links that terminate on the IPDS are down, try switching IPDS to hot-standby mate.		

Table 30-103 CmmLSS_externalConnectivity

Alarm	Attributes	Applicable major release
Name: CmmLSS_externalConnectivity (11416) Type: equipmentAlarm Package: ltecmm.CmmLSS_externalConnectivity Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: The system detected a problem or a state change to external connectivity.		
Remedial action: For INFO alarm, there is no action needed.For MAJOR and CRITICAL alarm, verify the cable connections from both HUB cards to customer layer 2 switches, check if the cables are plugged properly.For MAJOR and CRITIAL alarm, verify the port status on HUB cards, the port connect to the customer network should be in service.For MAJOR and CRITIAL alarm, verify the individual Ethernet port status on the HUB card for the given host with the alarm.For the CRITIAL alarm, verify connectivity to/from each of the IPs listed in the ARP list from the given host with the alarm.Check the next hop reported as failing. For a BFD session verify the router has the corresponding BFD session configured.Contact Customer Support for the correction procedure if above check can not correct it.		

Table 30-104 CmmLSS_externalLinkConfigurationLimit

Alarm	Attributes	Applicable major release
Name: CmmLSS_externalLinkConfigurationLimit (11417) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_externalLinkConfigurationLimit Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 17.0.0
Description: The maximum number of links for a given link type has been reached. When this limit is reached, it is not possible to create any new links of the given link type. Every 15 minutes a check will be performed in an attempt to recover any links which have not been used or have been disabled due to lack of far-end response. A configurable parameter, TdynMO , is used to control the aging algorithm for link recovery.		
Remedial action: Wait at least TdynMO time interval to allow the system to recover inactive or disabled links.If the system does not recover any links after TdynMO time interval, contact Customer Support.		

Table 30-105 CmmLSS_externalLinkDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_externalLinkDown (11418) Type: communicationsAlarm Package: ltecmm.CmmLSS_externalLinkDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: Communication between CMM and another network entity can not be established. The additional text field indicates the specific link that is down.		
Remedial action: Verify the network entity that CMM fails to communicate with is in service.Determine that there are no errors within the IP network.If the network entity data is provisioned on CMM, verify the data is correct.If multiple links that terminate on the IPDS are down, try switching IPDS to hot-standby mate.		

Table 30-106 CmmLSS_fcClientAppConfigErr

Alarm	Attributes	Applicable major release
Name: CmmLSS_fcClientAppConfigErr (11815) Type: processingErrorAlarm Package: ltecmm.CmmLSS_fcClientAppConfigErr Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0
Description: Missing TAI to LAI mapping configuration		
Remedial action: The service provider must make corrections to TAI-LAI mapping configuration data.Manually clear the alarm.		

Table 30-107 CmmLSS_fqdnError

Alarm	Attributes	Applicable major release
Name: CmmLSS_fqdnError (11419) Type: processingErrorAlarm Package: ltecmm.CmmLSS_fqdnError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: This alarm indicates the fully-qualified domain name (FQDN) DNS query error, as well as the Agent FQDN DNS query error.		
Remedial action: Verify the FQDN is correctly provisioned.Verify that FQDN is correctly provisioned on the external DNS server.Verify the FQDN is not provisioned with 0 IP address in DNS server.		

Table 30-108 CmmLSS_ggsnDnsError

Alarm	Attributes	Applicable major release
Name: CmmLSS_ggsnDnsError (11420) Type: processingErrorAlarm Package: ltecmm.CmmLSS_ggsnDnsError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: GGSN DNS Selection unable to retrieve IP Address. This alarm must be manually cleared.		
Remedial action: Verfiy that the GGSN IP Address is provisioned correctly on DNS server.Manually clear the alarm.		

Table 30-109 CmmLSS_hostReset

Alarm	Attributes	Applicable major release
Name: CmmLSS_hostReset (11816) Type: processingErrorAlarm Package: ltecmm.CmmLSS_hostReset Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0
Description: The Redundancy Manager is requesting a host reset. This will occur when one or more services on a host do not initialize properly and local recovery attempts have been unsuccessful.		
Remedial action: No manual action is needed for this alarm. It will be cleared automatically when services start to initialize.		

Table 30-110 CmmLSS_imConnectFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_imConnectFailure (11421) Type: processingErrorAlarm Package: ltecmm.CmmLSS_imConnectFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0
Description: This alarm indicates that the IM infrastructure failed to connect to an IM peer.		
Remedial action: Automatic retries to open the TCP socket connection will occur every 5 seconds.If the alarm does not automatically clear, proceed to step 2.Check configuration data such as FQDN, port and password.If the alarm does not automatically clear, proceed to step 3.Check whether IM server is in active state.If the alarm does not automatically clear, proceed to step 4.Initialize the service with IM infrastructure, such as IMS/CFED/DFED/AMC.If the alarm does not automatically clear, proceed to step 5.If the alarm does not clear, contact Customer Support.		

Table 30-111 CmmLSS_internalCommunicationFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_internalCommunicationFailure (11422) Type: communicationsAlarm Package: ltecmm.CmmLSS_ internalCommunicationFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: Communication between active IPDS member and active CPPS member failed or internal communications within active IPDS member failed.		
Remedial action: Verfiy IPDS and/or CPPS have not been forced out-of-service.If communication is lost between the CPPS and the IPDS and it does not come back automatically, and CPPS pool is in Active / Hot-standby state, try re-initializing CPPS member.If communiaction is lost between the IPDS and CPPS and it does not come back automatically, and IPDS pool is in Active / Hot-standby state, try switching IPDS to the standby member.		

Table 30-112 CmmLSS_ldapServerConnectionLost

Alarm	Attributes	Applicable major release
Name: CmmLSS_ldapServerConnectionLost (11423) Type: equipmentAlarm Package: ltecmm.CmmLSS_ ldapServerConnectionLost Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates an LDAP connection problem. The alarm severity will be critical if there is no connectivity to the LDAP server. Otherwise, the severity depends on whether the number of connections is deemed sufficient, based on data provisioned in the LDAP Server Interface Profile		
Remedial action: Verify configuration data in the LDAP Server Interface Profile. Check the status of the LDAP Server, DNS server, and communication network. FQDNs associated with the provisioned primary and/or secondary LDAP server URIs must be resolvable using DNS.Contact Customer Support, if needed.		

Table 30-113 CmmLSS_liNearingCapacityLimit

Alarm	Attributes	Applicable major release
Name: CmmLSS_liNearingCapacityLimit (11424) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_liNearingCapacityLimit Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: The number of lawful interceptions has reached 80% of CPPS capacity.		
Remedial action: Use the query option of the li_target_cli command to verify that the appropriate set of UEs are selected for lawful interception.		

Table 30-114 CmmLSS_linkMOStateChange

Alarm	Attributes	Applicable major release
Name: CmmLSS_linkMOStateChange (11425) Type: communicationsAlarm Package: ltecmm.CmmLSS_linkMOStateChange Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: Managed Object (MO) representing an CMM external link has changed state.		
Remedial action: No actions required.		

Table 30-115 CmmLSS_mariadbReplicationDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_mariadbReplicationDown (11426) Type: processingErrorAlarm Package: ltecmm.CmmLSS_mariadbReplicationDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomiz-ingError	Release: • 17.0.0
Description: The CMM uses the MariaDB database engine to store the 2G-3G-4G configuration data. This database is set up to run as a Master-Master configuration, with a replication link between the two nodes. This link will ensure the data updates on one node are propogated to the other node. It is possible that separate transactions can update the same data on both node simultaneously, causing failures to apply the data. In the event this occurs, the MariaDB replication link alarm is fired. Normally, the system will recover from most errors. However, if the corruption is severe, the alarm will persist, and service personal should be called to isolate the issue and possibly recover the database.		
Remedial action: CMM will recover itself, and clear the alarm for limited database failures. If the database failures are significant, the alarm will persist and support should be contacted to isolate the issue and recover the MariaDB database if required.Manually clear the alarm.		

Table 30-116 CmmLSS_memoryExhaustion

Alarm	Attributes	Applicable major release
Name: CmmLSS_memoryExhaustion (11427) Type: processingErrorAlarm Package: ltecmm.CmmLSS_memoryExhaustion Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpuCycleLimitExceeded	Release: • 17.0.0
Description: This alarm can be fired due to two different problems. The first field of 'Alarm Message' column in alarm will show the problem type.		
Remedial action: noSystemResourceAvailableMemory usage will fluctuate, and this problem may resolve itself quickly. However, if this is seen frequently, the processor may have experienced a problem because memory is not being freed properly; in this case, more drastic action may be required.For H248:Initialization of the cardKeep in mind that these actions may result in the loss of some calls. Switching over to standby process prior to this is advised. If this problem is seen repeatedly, Field support should be contacted.For CDR services:Initialization of the cardKeep in mind that these actions may result in the loss of some files. If this problem is seen repeatedly, field support should be contacted.utilizationReachedThresholdRe-establish the connection to CCF.		

Table 30-117 CmmLSS_memoryOverload

Alarm	Attributes	Applicable major release
Name: CmmLSS_memoryOverload (11428) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_memoryOverload Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: This alarm indicates the memory utilization on a diskless service has exceeded a threshold or a memory allocation failure has occured.The current default thresholds are: Minor - 80, Major - 85, Critical - 90.Note: for MM-SI AMMS service, the default thresholds are: Minor - 94, Major - 96, Critical - 98.		
Remedial action: If memory usage regularly exceeds thresholds, investigate how the call traffic load can be reduced.If it doesn't clear after step 1, contact Customer Support to check if there is memory leak occuring.		

Table 30-118 CmmLSS_mmeCallTraceStateChange

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeCallTraceStateChange (11429) Type: processingErrorAlarm Package: ltecmm.CmmLSS_ mmeCallTraceStateChange Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: The MME CPPS call trace software notify craft personel or management entities that a call trace job state change is detected. The valid call trace job states are 'pending', 'start' and 'stop'.		
Remedial action: None. This is only an informational alarm.		

Table 30-119 CmmLSS_mmeConnectionLost

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeConnectionLost (11817) Type: equipmentAlarm Package: ltecmm.CmmLSS_mmeConnectionLost Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm is raised whenever a MME (mobility management entity) disconnects with REM.		
Remedial action: Determine if its new growth MME but not setup connection with REM.If not then follow standard operating procedures for MME recovery.If the above steps do not clear the alarm, contact Customer Support.		

Table 30-120 CmmLSS_mmeControllerOOS

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeControllerOOS (11818) Type: equipmentAlarm Package: ltecmm.CmmLSS_mmeControllerOOS Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 17.0.0
Description: This alarm is raised whenever a SGS MME Controller goes out of service.		
Remedial action: Determine if the MME is in service on the LCP GUI, if not then put the MME into service if desired.Determine if the MME is in service. If not then follow local standard operating procedures for MME recovery.Determine if IP Connectivity exists both ways between MME and MSC. If not, then follow local standard operating procedures for IP Transport recovery.If the above steps do not clear the alarm, contact Customer Support.		

Table 30-121 CmmLSS_mmeDnsError

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeDnsError (11430) Type: processingErrorAlarm Package: ltecmm.CmmLSS_mmeDnsError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: MME DNS Selection unable to retrieve MME IP Address associated with FQDN. This alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.Manually clear the alarm.		

Table 30-122 CmmLSS_mmePcmdStateChange

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmePcmdStateChange (11431) Type: processingErrorAlarm Package: ltecmm.CmmLSS_mmePcmdStateChange Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: The CMM PCMD job has changed state.		
Remedial action: No actions required.		

Table 30-123 CmmLSS_mmeTAIeNBMapping

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeTAIeNBMapping (11432) Type: processingErrorAlarm Package: ltecmm.CmmLSS_mmeTAIeNBMapping Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0

Table 30-123 CmmLSS_mmeTAIeNBMapping (continued)

Alarm	Attributes	Applicable major release
Description: The MME uses a target TAI to route S1AP messages to a HeNB that is indirectly connected to the MME via a HeNB GW. In order for the MME to route a message to the correct HeNB GW, only one eNB that is directly connected to the MME can send the given TAI to the MME in an S1AP S1 Setup Request message. This alarm indicates that while routing an S1AP message via TAI, the MME detected that the TAI maps to more than one eNB. In this situation, the MME will attempt to route the message to one of the these eNBs. If that eNB cannot route the message further to a HeNB, the corresponding S1AP procedure is expected fail (e.g., S1 handover is rejected by that eNB). In order to remedy this situation, the service provider must modify eNB TAI configuration (using whatever configuration system is used by the eNB) so that only one eNB sends a given TAI to the MME. This alarm must be manually cleared after the service provider has made corrections to eNB configuration.		
Remedial action: The E-UTRAN service provider must modify eNB TAI configuration (using whatever configuration system is used by the eNB) so that only one eNB sends a given TAI to the MME.Manually clear the alarm.		

Table 30-124 CmmLSS_mmeTAInotSupported

Alarm	Attributes	Applicable major release
Name: CmmLSS_mmeTAInotSupported (11433) Type: processingErrorAlarm Package: ltecmm.CmmLSS_mmeTAInotSupported Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0
Description: The MME receives an eNB's supported TAIs in the S1AP S1 Setup Request and eNB Configuration Update messages. This alarm indicates that a TAI received from the eNB is not provisioned on the MME. In order to remedy this situation, the service provider must modify eNB TAI configuration (using whatever configuration system is used by the MME) or update the MME's configuration data to support the TAI indicated in the alarm. This alarm must be manually cleared after the service provider has made corrections to configuration data.		
Remedial action: The service provider must make corrections to either eNB or MME TAI configuration data.Manually clear the alarm.		

Table 30-125 CmmLSS_msgQueueResource

Alarm	Attributes	Applicable major release
Name: CmmLSS_msgQueueResource (11435) Type: processingErrorAlarm Package: ltecmm.CmmLSS_msgQueueResource Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: The alarm indicates that a resource has been exhausted in the course of program execution: Fixed length task's queue has become full and not capable of buffering an incoming message. Can not create a new queue as the maximum number of allowable queues has been reached		
Remedial action: There are no recovery actions that a craft can undertake to solve the problem stemming from the cause, as the problem is related to the configuration tables that come with a card binary image. Customer Support should be contacted.		

Table 30-126 CmmLSS_msThreshold

Alarm	Attributes	Applicable major release
Name: CmmLSS_msThreshold (11434) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_msThreshold Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: Number of attached MS or UE threshold reached		
Remedial action: If the problem persists, contact Customer Support.		

Table 30-127 CmmLSS_nodeManInhibit

Alarm	Attributes	Applicable major release
Name: CmmLSS_nodeManInhibit (11437) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_nodeManInhibit Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: quarantineMode	Release: • 17.0.0
Description: A command was specified to manually inhibit accepting new UEs to the system.		
Remedial action: To reset quarantine mode, enter the shutdown command at the UE load balancing command level.		

Table 30-128 CmmLSS_noResetAckReceived

Alarm	Attributes	Applicable major release
Name: CmmLSS_noResetAckReceived (11436) Type: communicationsAlarm Package: ltecmm.CmmLSS_noResetAckReceived Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: No RESET ACKNOWLEDGEMENT message was received from the RNC after the CMM has sent and resent a RESET message.		
Remedial action: Verify the RNC that CMM fails to get the message from with is in service.Determine that there are no errors within the IP network.		

Table 30-129 CmmLSS_numberOfTuplesInUse

Alarm	Attributes	Applicable major release
Name: CmmLSS_numberOfTuplesInUse (11438) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_numberOfTuplesInUse Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0

Table 30-129 CmmLSS_numberOfTuplesInUse (continued)

Alarm	Attributes	Applicable major release
Description: The raised alarm LSS_numberOfTuplesInUse indicates that the number of tuples currently in use in a DA (data access) table used to store dynamic database information, has reached a threshold. The DA table in question is specified in the 'Resource'. The threshold is indicated in the 'Additional Information'.Notes:A DA table can have the following thresholds:Minor Alarm OnsetMinor Alarm AbatementMajor Alarm OnsetMajor Alarm AbatementCritical Alarm OnsetCritical Alarm AbatementThe alarm will be raised (or will transition to a higher severity if already raised) if the number of tuples in use is greater than or equal to the onset threshold for that severity (specific to that table).The alarm will transition to a lower severity (or will be cleared if the current severity is minor) if the number of tuples in use is less than or equal to the abatement threshold for that severity (specific to that table).		
Remedial action: Contact Customer Support.		

Table 30-130 CmmLSS_pathAvailability

Alarm	Attributes	Applicable major release
Name: CmmLSS_pathAvailability (11439) Type: communicationsAlarm Package: ltecmm.CmmLSS_pathAvailability Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm is raised when SCTP path becomes unavailable. The local and remote provisioned addresses need to be checked for use of the correct 2 sub-networks provided. If the provisioned addresses match the 2 physical subnets, and if all address provisioned are also correct, then the physical network that carries the subnet used in the path 'unavailable' alarm needs to be investigated for trouble. The 'additionalText' field of the alarm indicates the type(s1mme, s11, etc.) of link that has a path down. To retrive which paths are down use the appropriate CLI command to retrieve path status. These alarms may need to be cleared manually: as alarms are reported when path connectivity is established, however their contents are a function of provisioned addresses (paths) that may be wrong and changed when the connection is down, and may no longer match with the path that was originally alarmed.Note: this alarm is cleared when the path's SCTP association changes operational state, either from 'Enabled' to 'Disabled' or from 'Disabled' to 'Enabled'. This change could result from an administrative lock or unlock action, or a change in the collective availability of the association's paths. Any path unreachable alarms will be cleared. If the new association state is 'Disabled', a single link/association alarm (LSS_externalLinkDown) will be raised.		
Remedial action: Verify that the endpoints IP addresses on the CMM are the remote entity are provisioned correctly.Verify that the network between the CMM and the remote entity is functioning correctly.		

Table 30-131 CmmLSS_pgwDnsError

Alarm	Attributes	Applicable major release
Name: CmmLSS_pgwDnsError (11441) Type: processingErrorAlarm Package: ltecmm.CmmLSS_pgwDnsError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: CMM DNS Selection unable to retrieve PGW IP Address associated with FQDN. This alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.Manually clear the alarm.		

Table 30-132 CmmLSS_processDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_processDown (11442) Type: equipmentAlarm Package: ltecmm.CmmLSS_processDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentMalfunction	Release: • 17.0.0
Description: This alarm indicates that an application process that should be running has terminated.		
Remedial action: Recovery software should automatically recover from the abnormal or maintenance event that has caused the process termination, without any manual involvement. The automatic recovery will restart just that process or will reboot the card as necessary.If the alarm does not clear or if it occurs repeatedly, contact Customer Support.		

Table 30-133 CmmLSS_processNotStarted

Alarm	Attributes	Applicable major release
Name: CmmLSS_processNotStarted (11443) Type: processingErrorAlarm Package: ltecmm.CmmLSS_processNotStarted Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: The processNotStarted alarm is caused if an application process cannot be started, or one of the following daemons has a problem starting:ipmunboundsshd (on all service hosts with fixed IP address)ntpd (on all service hosts on non-CPSB platforms)		
Remedial action: IPM: Based on the type of failure encountered, recovery actions may vary. If the ipmStartupFailure is generated, contact Customer Support. Once the failure is corrected, the startup of the ipm process will automatically clear the alarm.UNBOUND: Based on the type of failure encountered, recovery actions may vary. If the unboundStartupFailure is generated, contact Customer Support. Once the failure is corrected, the startup of the unbound process will automatically clear the alarm.SSHD: Based on the type of failure encountered, recovery actions may vary. If the sshdStartupFailure is generated, contact Customer Support. Once the failure is corrected, the startup of the sshd process will automatically clear the alarm.NTPD: Based on the type of failure encountered, recovery actions may vary. If the ntpdStartupFailure is generated, contact Customer Support. Once the failure is corrected, the startup of the ntpd process will automatically clear the alarm.Application Process: Based on the type of failure encountered, recovery actions may vary. If the applStartupFailure is generated, contact Customer Support. Once the failure is corrected, the startup of the application process will automatically clear the alarm.		

Table 30-134 CmmLSS_progressMarker

Alarm	Attributes	Applicable major release
Name: CmmLSS_progressMarker (11444) Type: processingErrorAlarm Package: ltecmm.CmmLSS_progressMarker Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: This alarm is an indication of (re)initialization/(re)configuration progression for a REM controlled service.		
Remedial action: No actions required. When the initialization/configuration of the card completes, there will be no further (progress marker) alarms for this service.		

Table 30-135 CmmLSS_provisioningError

Alarm	Attributes	Applicable major release
Name: CmmLSS_provisioningError (11819) Type: processingErrorAlarm Package: ltecmm.CmmLSS_provisioningError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomizingError	Release: • 17.0.0
Description: Missing provisioning of TAI-to-LAI mapping to MSC in 2G/3G operator for SGS based CSFB/SMS.		
Remedial action: Provision missing entries in TAI-LAI mapping table utilizing LAI in 2G/3G operator. Refer to user text in alarm.		

Table 30-136 CmmLSS_remotedbLinkDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_remotedbLinkDown (11445) Type: processingErrorAlarm Package: ltecmm.CmmLSS_remotedbLinkDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: This alarm will be displayed when the remotedb trigger function connection does not exist.		
Remedial action: Normally the alarm will be cleared automatically when a remote service restarts and re-connects to the remotedb database; If this alarm is not cleared, please contact Customer Support.		

Table 30-137 CmmLSS_sctpEndpointInactive

Alarm	Attributes	Applicable major release
Name: CmmLSS_sctpEndpointInactive (11446) Type: communicationsAlarm Package: ltecmm.CmmLSS_sctpEndpointInactive Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protectionPathFailure	Release: • 17.0.0
Description: The CMM provisioning for this remote endpoint is for SCTP multi-homing (multiple IP addresses). Upon establishment of the SCTP association, the CMM has detected that the provisioned IP Address indicated is inactive (is not being used by the SCTP association).		
Remedial action: Find the CMM Iu-PS or Gr link corresponding to the indicated IP address.Determine whether or not the CMM provisioned IP address is correct for this remote endpoint.Verify that there are no errors within the IP network.		

Table 30-138 CmmLSS_sctpPriPathInconsistency

Alarm	Attributes	Applicable major release
Name: CmmLSS_sctpPriPathInconsistency (11820) Type: processingErrorAlarm Package: ltecmm.CmmLSS_sctpPriPathInconsistency Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: datebaseInconsistency	Release: • 17.0.0
Description: This alarm indicates the primary SCTP destinaion that user wants to manually set is different from preferred primary destination that user already configured.		
Remedial action: Manually set the primary SCTP destination back to preferred primary destination configured.		

Table 30-139 CmmLSS_serviceCommCxnLost

Alarm	Attributes	Applicable major release
Name: CmmLSS_serviceCommCxnLost (11447) Type: equipmentAlarm Package: ltecmm.CmmLSS_serviceCommCxnLost Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm is generated when the connection established using serviceComm between services is lost.		
Remedial action: The alarm clears automatically when the connection is reestablished.		

Table 30-140 CmmLSS_sgsnDnsError

Alarm	Attributes	Applicable major release
Name: CmmLSS_sgsnDnsError (11448) Type: processingErrorAlarm Package: ltecmm.CmmLSS_sgsnDnsError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: SGSN DNS Selection unable to retrieve SGSN IP Address associated with FQDN. This alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.Manually clear the alarm.		

Table 30-141 CmmLSS_sgwResourceDegraded

Alarm	Attributes	Applicable major release
Name: CmmLSS_sgwResourceDegraded (11449) Type: communicationsAlarm Package: ltecmm.CmmLSS_sgwResourceDegraded Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: The raised LSS_sgwResourceDegraded alarm indicates the CMM selection on SGW or SGW-PGW pair has been degraded.		

Table 30-141 CmmLSS_sgwResourceDegraded (continued)

Alarm	Attributes	Applicable major release
Remedial action: Determine that there are no errors within the IP network.Determine that the SGW and/or SGW PGW pair are in service.Check if the invocation of CLI was intentional.Alarms are cleared when SGW and/or SGW PGW pair MOs are resumed. If the SGW and/or SGW PGW pair is suspended manually, then the alarm can only be cleared when the SGW and/or SGW PGW MO are resumed manually via CLI.		

Table 30-142 CmmLSS_sheddingOverload

Alarm	Attributes	Applicable major release
Name: CmmLSS_sheddingOverload (11450) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_sheddingOverload Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: This alarm indicates the message shedding severity under system overload. The two severity levels indicate the degree of shedding severity.The types of messages/calls that are shed is specific to the application and there tends to be additional types of messages impacted by the shedding as the severity increases. Currently the default thresholds between Major and Critical is 70.		
Remedial action: Verify that there is no running debug or testing tool that uses a lot of CPU/memory.If CPU or memory utilization regularly exceeds thresholds, investigate how the call traffic load can be reduced:Reengineer so less traffic is directed to this office or card.Consider replacing the overloaded card pair with higher-capacity cards.Verify if there are enough cards to handle the expected load and add additional cards as appropriate.		

Table 30-143 CmmLSS_softwareAllocatedResourceOverload

Alarm	Attributes	Applicable major release
Name: CmmLSS_softwareAllocatedResourceOverload (11451) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_ softwareAllocatedResourceOverload Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceAtOrNearingCapacity	Release: • 17.0.0
Description: This alarm indicates that the utilization of a pre-allocated resource by software has exceeded thresholds. The resource could be internal buffer, data structure array, table entries, etc.		
Remedial action: Consider reengineering so that less traffic is directed to this service.If condition persists, contact Customer Support.		

Table 30-144 CmmLSS_swVersionMismatch

Alarm	Attributes	Applicable major release
Name: CmmLSS_swVersionMismatch (11452) Type: processingErrorAlarm Package: ltecmm.CmmLSS_swVersionMismatch Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 17.0.0

Table 30-144 CmmLSS_swVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The software version running on this service member does not match the version that should be running according to the database table IPCFG_POOL_MEMBERS, field build_sec.		
Remedial action: Contact Customer Support.		

Table 30-145 CmmLSS_taiFqdnError

Alarm	Attributes	Applicable major release
Name: CmmLSS_taiFqdnError (11453) Type: processingErrorAlarm Package: ltecmm.CmmLSS_taiFqdnError Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareError	Release: • 17.0.0
Description: MME DNS Selection unable to retrieve SGW IP Address associated with FQDN. this alarm must be manually cleared.		
Remedial action: Verify that the FQDN is provisioned correctly in DNS server.Manually clear the alarm.		

Table 30-146 CmmLSS_tcpDown

Alarm	Attributes	Applicable major release
Name: CmmLSS_tcpDown (11454) Type: equipmentAlarm Package: ltecmm.CmmLSS_tcpDown Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm is used by UMTS and IMS applications. Alarm information is given under application specific sub-section below.UMTS applicationThis alarm will be displayed if CDR logger process loses connection to mate CDR logger process in a duplex CDR Host configuration, or if CDR logger process loses connection to local CDR receiver process.IMS applicationThis alarm will be displayed if diameter connection to CCF is failed and some criteria is met, or if iCCF receiver process loses connection to mate iCCF receiver process in a duplex CDR services configuration, or if iCCF logger process loses connection to mate iCCF logger process, or if iCCF logger process loses connection to local iCCF receiver process.		
Remedial action: Check and fix if there are issues with connectivity. If alarm still persists, contact Customer Support.		

Table 30-147 CmmLSS_threadsExhausted

Alarm	Attributes	Applicable major release
Name: CmmLSS_threadsExhausted (11455) Type: processingErrorAlarm Package: ltecmm.CmmLSS_threadsExhausted Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpuCycleLimitExceeded	Release: • 17.0.0
Description: One or more critical CP Tasks have been un-responsive to regular Integrity Monitor - IMON Heartbeats. IMON attempted to restart them and multiple restarts have escalated to a Process Init on the Standby Card or a Switch Over to the Standby Card from the Active Card where the target stuck task was running.		

Table 30-147 CmmLSS_threadsExhausted (continued)

Alarm	Attributes	Applicable major release
Remedial action: NOT APPLICABLE		

Table 30-148 CmmLSS_tunnelMonitorHeartbeatFailure

Alarm	Attributes	Applicable major release
Name: CmmLSS_tunnelMonitorHeartbeatFailure (11456) Type: equipmentAlarm Package: ltecmm.CmmLSS_ tunnelMonitorHeartbeatFailure Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkFailure	Release: • 17.0.0
Description: This alarm indicates that the process tmon lost heartbeat with the far end gateway IP.		
Remedial action: Check the physical connection between far end gateway and the blade where tmon is running and make sure all the configuration(on both LCP and the far end gateway) is correct.This alarm will be cleared if the heartbeat recovers.Contact Customer Support if the alarm is generated frequently.		

Table 30-149 CmmLSS_vLRHostIPconnectionOOS

Alarm	Attributes	Applicable major release
Name: CmmLSS_vLRHostIPconnectionOOS (11457) Type: processingErrorAlarm Package: ltecmm.CmmLSS_ vLRHostIPconnectionOOS Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: This alarm is raised whenever an IP connection between a VLR (visitor location register) Host and a Device Server/Call Server goes out of service.		
Remedial action: Determine if the ESC is in service. If not then follow the procedures for ESC recovery.Determine if the VLR Host is in service. If not then follow the procedures for Host recovery.Determine if the mapsys process is running on the VLR Host. If not then follow the procedures for VLR service recovery.Determine if the Device Server/Call Server is in service. If not then follow the procedures for Device Server/Call Server recovery.If the above steps do not clear the alarm, contact Customer Support.		

Table 30-150 CmmLSS_vmOverload

Alarm	Attributes	Applicable major release
Name: CmmLSS_vmOverload (11458) Type: qualityOfServiceAlarm Package: ltecmm.CmmLSS_vmOverload Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • 17.0.0
Description: This alarm indicates the virtual memory size of an application process has exceeded a threshold.		

Table 30-150 CmmLSS_vmOverload (continued)

Alarm	Attributes	Applicable major release
Remedial action: Contact Customer Support to check if there is memory leak occuring.		

Table 30-151 CmmSystemServiceUnavailable

Alarm	Attributes	Applicable major release
Name: CmmSystemServiceUnavailable (11822) Type: equipmentAlarm Package: ltecmm.CmmSystemServiceUnavailable Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: serviceError	Release: • 17.0.0
Description: system service unavailablesystemd process has noticed that service has been stopped or failed.		
Remedial action: System cancels this alarm automatically when the fault has been recovered. This alarm can be also cancelled via O&M interfaces.		

Table 30-152 CmmUnknownAlarm

Alarm	Attributes	Applicable major release
Name: CmmUnknownAlarm (11461) Type: processingErrorAlarm Package: ltecmm.CmmUnknownAlarm Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unspecifiedReason	Release: • 17.0.0
Description: The alarm is raised when an unknown alarm is received from the CMM system.		
Remedial action: Obtain the native CMM alarm name from the additional text field. Open the Nokia-CMM MI GUI and locate the corresponding CMM alarm. Refer to the Fault Clearance Procedure in the help documentation for the alarm.		

Table 30-153 CmmVmUnreachable

Alarm	Attributes	Applicable major release
Name: CmmVmUnreachable (11823) Type: equipmentAlarm Package: ltecmm.CmmVmUnreachable Raised on class: ltecmm.CmmAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: vmDown	Release: • 17.0.0
Description: VM unit does not respond to unit alive checkVM unit is down or alive checking does not work correctly		
Remedial action: check status of vm units		

Table 30-154 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 17.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 30-155 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 30-156 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 30-157 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 30-158 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 17.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 30-159 criticalErrorAlarm (ltecmm)

Alarm	Attributes	Applicable major release
Name: criticalErrorAlarm (3681) Type: communicationsAlarm Package: ltecmm.criticalErrorAlarm Raised on class: ltecmm.CMMInstance	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CMMInternalProcessingError	Release: • 17.0.0
Description: This alarm is raised when receiving critical-error message from the network element's NETCONF interface. The operator must connect to the network element using its CLI interface and verify the consistency of the network element's database and configuration and then do a full node resync once the manual intervention has been completed.		

Table 30-159 criticalErrorAlarm (ltecmm) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operator must connect to the network element (CMM) using its CLI interface and verify the consistency of the network element's database and configuration and then do a full node resync once the manual intervention has been completed.		

Table 30-160 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 17.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 30-161 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 30-162 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		

Table 30-162 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 30-163 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 17.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 30-164 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 30-165 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 17.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 30-166 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 17.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 30-167 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 17.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 30-167 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 30-168 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 17.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 30-169 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 17.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 30-170 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 17.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 30-171 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 30-172 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 17.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 30-172 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 30-173 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 17.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 30-174 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 17.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 30-175 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 17.0.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 30-176 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 30-177 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 17.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		

Table 30-177 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 30-178 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 17.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 30-179 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 17.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 30-180 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 30-181 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 17.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 30-182 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 17.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 30-183 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 17.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 30-184 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 17.0.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 30-185 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 17.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 30-186 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 30-187 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 30-188 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 17.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 30-188 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 30-189 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 17.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 30-190 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 17.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 30-190 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 30-191 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 17.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 30-192 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 17.0.0

Table 30-192 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 30-193 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 17.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 30-194 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 17.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 30-195 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 17.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 30-196 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 17.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 30-197 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 17.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 30-198 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 17.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 30-199 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 17.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

31 7850 VSG

31.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 31-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 31-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 31-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 31-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 31-4 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 31-5 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 31-6 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 31-7 AsymmetricalConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: multichassis.AsymmetricalConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.AbstractMultiChassisPeer • multichassis.AbstractMultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 4.0
Description: The alarm is raised when there is a peer configuration mismatch that prevents MC operation.		
Raising condition: ('Config Mismatches' NOT EQUAL '0L')		
Clearing condition: ('Config Mismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 31-8 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 31-9 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-9 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 31-10 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 31-11 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		

Table 31-11 BgpDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-12 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 31-13 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 31-14 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 31-15 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 31-16 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-16 BITSNotQualified (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 31-17 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 31-18 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 31-19 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPol-lInRange	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 31-20 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 31-21 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 31-22 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 31-23 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 31-24 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 31-25 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 31-26 ConfigurationRescueFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileDeleteStatus (3894) Type: configurationRescueAlarm Package: rollback. ConfigurationRescueFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileDeleteOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback rescue file delete operation is performed.		
Remedial action: Informational - If rollback rescue file deletion status indicates failed, then, the requested rescue file might not be available or check the FTP permission for the rescue location.		

Table 31-27 ConfigurationRescueFileSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueFileSaveStatus (3895) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueFileSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueFileSaveOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback rescue save operation is performed.		

Table 31-27 ConfigurationRescueFileSaveStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - If rollback rescue file creation status indicates failed, then, check the FTP permission for the rescue location.		

Table 31-28 ConfigurationRescueStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRescueStatus (3896) Type: configurationRescueAlarm Package: rollback.ConfigurationRescueStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRescueOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback rescue operation is performed.		
Remedial action: Informational - If rollback rescue status indicates failed, then, the rescue file might not be available or check the FTP permission for the rescue location.		

Table 31-29 ConfigurationRollBackFileDeleteStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileDeleteStatus (3897) Type: configurationRollBackAlarm Package: rollback. ConfigurationRollBackFileDeleteStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileDeleteOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback file delete operation is performed.		
Remedial action: Informational - If rollback file deletion status indicates failed, then, the requested rollback file might not be available or check the FTP permission for the rollback location..		

Table 31-30 ConfigurationRollBackFileSyncStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackFileSyncStatus (3898) Type: configurationRollBackFileSyncAlarm Package: rollback.ConfigurationRollBackFileSyncStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackFileSyncOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback CPM sync operation is performed.		
Remedial action: Informational - If rollback files CPM Sync status indicates failed, then, check whether standby CPM is up.		

Table 31-31 ConfigurationRollBackSaveStatus

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackSaveStatus (3899) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackSaveStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackSaveOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback save operation is performed.		
Remedial action: Informational - If rollback file creation status indicates failed, then, check the FTP permission for the rollback location.		

Table 31-32 ConfigurationRollBackStatus (rollback)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: rollback.ConfigurationRollBackStatus Raised on class: rollback.RollbackNEInfo	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 31-33 ConfigurationRollBackStatus (netw)

Alarm	Attributes	Applicable major release
Name: ConfigurationRollBackStatus (3684) Type: configurationRollBackAlarm Package: netw.ConfigurationRollBackStatus Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationRollBackOperationPerformed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration rollback operation is performed.		
Remedial action: Informational - If rollback status indicates failed, then, the requested checkpoint might not be available or NE configuration might need to be restored.		

Table 31-34 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 31-35 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		

Table 31-35 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 31-36 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 31-37 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 31-37 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 31-38 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-39 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-40 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-41 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtViolPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-42 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-42 CpmProtectionViolationSAPEntry (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-43 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 31-44 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 31-45 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec. CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 31-46 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-47 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-47 DDMAux1HighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-48 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-49 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-50 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-51 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-52 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-52 DDMAux2LowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-53 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-54 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-55 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-56 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-57 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-57 DDMRxOpticalPowerLowWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-58 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-59 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-60 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-61 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-62 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-62 DDMTemperatureHighAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-63 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-64 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-65 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-66 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-67 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-67 DDMTxBiasCurrentHighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-68 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-69 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-70 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-71 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-72 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-72 DDMTxOutputPowerLowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-73 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 31-74 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 31-75 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 31-76 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 31-77 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-77 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 31-78 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-79 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		

Table 31-79 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 31-80 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 31-81 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 31-82 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 31-83 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 31-84 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 31-85 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 31-86 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 31-87 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 31-88 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 31-89 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 31-90 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 31-91 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 31-92 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 31-93 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 31-94 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-94 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 31-95 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 31-96 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		

Table 31-96 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 31-97 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 31-98 IgmpMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpMaxSrcsLimitExceeded (3742) Type: configurationAlarm Package: igmp.IgmpMaxSrcsLimitExceeded Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpMaxSrcsLimitExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an attempt is made to configure an IGMP source for a group when the number of sources for this group is equal to 'maxSources', the maximum number of sources per group supported on the interface.		
Remedial action: Needs to increase 'maxSources' value to allow more sources on this interface.		

Table 31-99 IncompleteConfig (multichassis)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: multichassis.IncompleteConfig Raised on classes: • multichassis.MultiChassisLagMember • multichassis.MultiChassisSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 4.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('mcLagPointer' EQUAL '\"\"')		
Clearing condition: ('mcLagPointer' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered object.		

Table 31-100 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 31-101 IncorrectEndPointPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectEndPointPeerConfig (1068) Type: configurationAlarm Package: multichassis.IncorrectEndPointPeerConfig Raised on class: multichassis.MultiChassisEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteEPPeerConfig	Release: • 4.0
Description: The alarm is raised when a peer configuration cannot be found on the peer NE.		
Raising condition: ('MC EndPoint Group Pointer' EQUAL '\"\"')		

Table 31-101 IncorrectEndPointPeerConfig (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('MC EndPoint Group Pointer' NOT EQUAL '\"\"')		
Remedial action: The peered object cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 31-102 IncorrectPeerConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerConfig (779) Type: configurationAlarm Package: multichassis.IncorrectPeerConfig Raised on class: multichassis.AbstractPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerConfig	Release: • 4.0
Description: The alarm is raised when an MC peer does not exist, or when an MC peer exists but the peer address is not the address of a network interface on the peer.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: The peer configuration cannot be found on the peer NE. Either delete this one, or create the missing peer object.		

Table 31-103 IncorrectPeerSynchronizationPortConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronizationPortConfig (780) Type: configurationAlarm Package: multichassis. IncorrectPeerSynchronizationPortConfig Raised on class: multichassis. PeerSynchronizationPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortConfig	Release: • 4.0
Description: The alarm is raised when the peer port does not exist, or when the peer port exists but the synchronization tags of the peers do not match.		
Raising condition: ('peerMatchFound' EQUAL 'false')		
Clearing condition: ('peerMatchFound' EQUAL 'true')		
Remedial action: Check if the peer port does not exist, or the peer port exists but the synchronization tags do not match.		

Table 31-104 IncorrectPeerSynchronizationPortEncapRangeConfig

Alarm	Attributes	Applicable major release
Name: IncorrectPeerSynchronization-PortEncapRangeConfig (781) Type: configurationAlarm Package: multichassis.IncorrectPeerSynchronizationPortEncapRangeConfig Raised on class: multichassis.PeerSynchronizationPortEncapRange	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncorrectPeerSynchronization-PortEncapRangeConfig	Release: • 4.0
Description: The alarm is raised when the VLAN ranges on the Multi-Chassis synchronization peers do not match.		
Raising condition: ('Neighbor Match' EQUAL 'false')		
Clearing condition: ('Neighbor Match' EQUAL 'true')		
Remedial action: Update the VLAN ranges on the Multi-Chassis synchronization peers to make them matching.		

Table 31-105 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 31-106 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-106 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 31-107 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 31-108 InterfaceNeighborDown

Alarm	Attributes	Applicable major release
Name: InterfaceNeighborDown (661) Type: NeighborDown Package: ospf.InterfaceNeighborDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an interface neighbor is operationally down.		
Raising condition: (('Neighbor Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'true'))		

Table 31-108 InterfaceNeighborDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Neighbor Count' NOT EQUAL '0L') OR ('Passive' EQUAL 'true'))		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-109 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 31-110 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 31-111 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 31-112 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 31-113 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 31-114 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 31-115 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 31-116 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 31-117 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-117 LdpSessionNonexistent (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 31-118 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 31-119 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 31-120 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 31-121 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 31-122 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 31-123 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 31-124 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 31-125 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 31-126 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-126 macMoveRateExceeded (service) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 31-127 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 31-128 MCLagDown (multichassis)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: multichassis.MCLagDown Raised on class: multichassis. MultiChassisLagPeerSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 4.0
Description: The alarm is raised when all ports in an MC LAG are operationally Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 31-129 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 31-130 MCPeerEPDown

Alarm	Attributes	Applicable major release
Name: MCPeerEPDown (1069) Type: equipmentAlarm Package: multichassis.MCPeerEPDown Raised on class: multichassis.MultiChassisEndpoint	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MCPeerEPDown	Release: • 4.0
Description: The alarm is raised when an MC endpoint is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Bring up the all End Point Members.		

Table 31-131 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-131 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 31-132 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 31-133 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 31-133 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 31-134 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 31-135 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 31-136 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 31-137 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 31-138 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 31-139 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 31-140 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 31-141 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 31-142 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-142 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-143 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 31-144 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 31-145 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 31-146 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 31-147 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 31-148 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		

Table 31-148 NodeSuspended (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 31-149 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 31-150 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 31-151 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-152 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 31-153 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 31-154 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 31-155 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 31-156 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 31-157 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-158 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-159 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 31-160 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 31-161 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 31-162 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol- dExceededAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 31-163 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 31-164 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-165 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-166 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-167 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-168 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 31-169 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-170 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-171 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 31-172 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 31-173 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 31-174 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 31-175 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 31-176 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 31-177 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-177 PTPReferenceOutOfPollInRange (sonet) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 31-178 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 31-179 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 31-179 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 31-180 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 31-181 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 31-182 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 31-183 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 31-184 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 31-185 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 31-186 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 31-187 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 31-188 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 31-189 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 31-190 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 31-191 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 31-192 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 31-193 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 31-194 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 31-195 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 31-196 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-197 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 31-198 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 31-199 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 31-200 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-200 SpbSiteDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 31-201 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 31-202 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 31-202 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 31-203 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 31-204 svcMacFdbTabelFull

Alarm	Attributes	Applicable major release
Name: svcMacFdbTabelFull (3890) Type: resourceAlarm Package: netw.svcMacFdbTabelFull Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the system limit of FDB records is reached.		
Remedial action: The alarm is raised when system limit of FDB records is reached.		

Table 31-205 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 31-206 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 31-207 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 31-208 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 31-208 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 31-209 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 31-210 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 31-211 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 31-212 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-212 TunnelDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 31-213 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 31-214 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 31-215 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 31-216 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 31-217 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 31-217 upgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 31-218 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 31-219 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 31-220 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 31-221 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-222 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 31-223 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 31-224 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

32 DC VSA-8

32.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 32-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 32-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 3.2 • 4.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 32-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 3.2 • 4.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 32-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 32-5 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		

Table 32-5 AncillaryPathLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 32-6 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 3.2 • 4.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 32-7 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 3.2 • 4.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 32-8 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 32-9 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 3.2 • 4.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 32-10 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-11 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 32-12 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 32-13 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 32-14 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 32-15 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 32-16 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 32-17 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 32-18 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 3.2 • 4.0
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 32-19 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 32-19 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 32-20 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 32-21 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 32-22 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 3.2 • 4.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 32-23 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 32-24 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 32-25 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 32-26 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 32-27 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 32-27 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 32-28 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 3.2 • 4.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 32-29 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-30 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-31 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-32 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtVioIPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-33 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtViolSapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-34 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 32-35 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 32-36 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec.CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 32-37 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-38 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-39 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-40 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-41 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-42 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-43 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-44 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-45 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-46 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment. DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-47 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-48 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-49 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-50 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-51 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-52 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-53 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-54 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-55 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-56 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-57 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-58 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-59 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-60 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-61 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-62 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-63 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-64 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 32-65 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 3.2 • 4.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 32-66 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 32-67 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 32-68 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 32-69 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-70 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 3.2 • 4.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 32-71 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		

Table 32-71 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 32-72 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 32-73 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 3.2 • 4.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 32-74 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 32-75 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 32-76 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		

Table 32-76 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 32-77 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 32-78 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 32-79 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 32-80 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 32-81 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		

Table 32-81 EthernetPortSignalFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 32-82 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 3.2 • 4.0
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 32-83 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 32-84 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 3.2 • 4.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 32-85 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 3.2 • 4.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 32-86 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		

Table 32-86 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 32-87 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 32-88 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 32-89 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 3.2 • 4.0

Table 32-89 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 32-90 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 32-91 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 32-92 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 32-93 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 32-94 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 32-95 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 32-96 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 32-97 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 3.2 • 4.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		

Table 32-97 LabelProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 32-98 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 3.2 • 4.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 32-99 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 32-100 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 32-101 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 32-102 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 32-103 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 3.2 • 4.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 32-104 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 3.2 • 4.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 32-105 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 3.2 • 4.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 32-106 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 32-107 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 32-108 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 3.2 • 4.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 32-109 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 32-110 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 3.2 • 4.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 32-111 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 3.2 • 4.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 32-112 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 3.2 • 4.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 32-113 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 3.2 • 4.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 32-114 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 3.2 • 4.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		

Table 32-114 MissingLocalEntry (continued)

Alarm	Attributes	Applicable major release
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 32-115 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 32-116 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 32-117 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 3.2 • 4.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 32-118 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 3.2 • 4.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 32-119 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 3.2 • 4.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 32-120 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 32-121 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 3.2 • 4.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 32-122 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 3.2 • 4.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 32-123 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 32-124 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		

Table 32-124 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 32-125 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 3.2 • 4.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 32-126 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 32-127 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 3.2 • 4.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 32-128 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 3.2 • 4.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 32-129 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 32-130 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 32-131 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 3.2 • 4.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 32-132 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 32-133 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 32-134 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 32-135 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 3.2 • 4.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		

Table 32-135 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 32-136 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 32-137 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 32-138 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-139 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-140 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 3.2 • 4.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		

Table 32-140 PeerLacIngressEgressFault (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 32-141 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 32-142 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 32-143 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 32-144 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 32-145 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 3.2 • 4.0
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		

Table 32-145 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-146 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 3.2 • 4.0
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-147 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-148 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 3.2 • 4.0

Table 32-148 PowerSupplyInputFailure (continued)

Alarm	Attributes	Applicable major release
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-149 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 3.2 • 4.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 32-150 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 3.2 • 4.0
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-151 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 3.2 • 4.0
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-152 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 3.2 • 4.0
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 32-153 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 3.2 • 4.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 32-154 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 32-155 PTPNotQualified

Alarm	Attributes	Applicable major release
Name: PTPNotQualified (3611) Type: communicationsAlarm Package: sonet.PTPNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPNotQualified	Release: • 3.2 • 4.0
Description: The alarm is raised when PTP on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 32-156 PTPReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: sonet.PTPReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • 3.2 • 4.0
Description: The alarm is raised when the PTP reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 32-157 PTPReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • 3.2 • 4.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 32-158 PTPReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: sonet.PTPReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • 3.2 • 4.0
Description: The alarm is raised when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 32-159 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 3.2 • 4.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 32-160 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 32-161 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 3.2 • 4.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 32-162 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 3.2 • 4.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		

Table 32-162 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 32-163 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 3.2 • 4.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 32-164 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 3.2 • 4.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 32-165 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 3.2 • 4.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 32-166 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 3.2 • 4.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 32-167 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 3.2 • 4.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		

Table 32-167 S2LPathBypassTunnelActive (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 32-168 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 32-169 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 3.2 • 4.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 32-170 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		

Table 32-170 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 32-171 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 3.2 • 4.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 32-172 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 3.2 • 4.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 32-173 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 3.2 • 4.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 32-174 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 3.2 • 4.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 32-175 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 3.2 • 4.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		

Table 32-175 ServiceSiteDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 32-176 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 32-177 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 32-178 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 3.2 • 4.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 32-179 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 32-180 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 32-181 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 32-182 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 32-183 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 3.2 • 4.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 32-184 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 3.2 • 4.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 32-185 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 3.2 • 4.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 32-186 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 3.2 • 4.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		

Table 32-186 TmnxEqPortEtherLoopDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 32-187 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 32-188 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 3.2 • 4.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 32-188 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 32-189 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 3.2 • 4.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 32-190 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 3.2 • 4.0

Table 32-190 TunnelAdministrativelyDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 32-191 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 32-192 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 3.2 • 4.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 32-193 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 32-194 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 3.2 • 4.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 32-195 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 3.2 • 4.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 32-196 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 3.2 • 4.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 32-197 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 3.2 • 4.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 32-198 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 3.2 • 4.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 32-199 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 3.2 • 4.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 32-200 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 3.2 • 4.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 32-201 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 32-202 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 3.2 • 4.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 32-203 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 3.2 • 4.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 32-204 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 3.2 • 4.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		

Table 32-204 XplError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

33 VSC

33.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 33-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 33-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 33-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 33-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 33-4 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 33-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 33-6 AsymmetricalConfig (lag)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: lag.AsymmetricalConfig Raised on classes: • lag.MultiChassisLag • lag.MultiChassisLagMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the members of an MC LAG do not have matching configurations.		
Raising condition: ('configMismatches' NOT EQUAL '0L')		
Clearing condition: ('configMismatches' EQUAL '0L')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 33-7 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 33-8 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 33-9 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 33-10 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 33-11 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 33-12 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 33-13 CircuitStpExceptionCondition

Alarm	Attributes	Applicable major release
Name: CircuitStpExceptionCondition (648) Type: SdpBindingAlarm Package: l2fwd.CircuitStpExceptionCondition Raised on class: l2fwd.CircuitStp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: StpException	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an NE detects an STP exception condition on a SAP, for example, one-way communication or a downstream loop. The alarm clears when the STP status changes.		
Raising condition: (('STP Exception Condition' NOT EQUAL 'None') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('STP Exception Condition' EQUAL 'None') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Check 'STP Exception Condition' field for more details and fix the STP exception.		

Table 33-14 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 33-15 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 33-16 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 33-17 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-17 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 33-18 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 33-19 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 33-19 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 33-20 CpmProtectionExceedEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedEntry (2925) Type: communications Package: sitesec.CpmProtectionExceedEntry Raised on class: sitesec.CpmProtExcdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MAC packet stream has exceeded its per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-21 CpmProtectionExceedSapIpEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionExceedSapIpEntry (3911) Type: communications Package: sitesec.CpmProtectionExceedSapIpEntry Raised on class: sitesec.CpmProtExcdSapIpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IP packet stream has exceeded the per-source limit.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-22 CpmProtectionViolationIfEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationIfEntry (2926) Type: communications Package: sitesec.CpmProtectionViolationIfEntry Raised on class: sitesec.CpmProtVioIfEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the interface is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-23 CpmProtectionViolationPortEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationPortEntry (2927) Type: communications Package: sitesec.CpmProtectionViolationPortEntry Raised on class: sitesec.CpmProtVioIPortEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the link-specific packet arrival rate limit at the port is violated.		
Raising condition: (('Number of Per-port Violations' NOT EQUAL '0L') OR ('Number of Link-specific Violations' NOT EQUAL '0L'))		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-24 CpmProtectionViolationSAPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSAPEntry (2928) Type: communications Package: sitesec.CpmProtectionViolationSAPEntry Raised on class: sitesec.CpmProtVioISapEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-24 CpmProtectionViolationSAPEntry (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the link-specific packet arrival rate limit at the SAP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-25 CpmProtectionViolationSDPEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationSDPEntry (5415) Type: communications Package: sitesec.CpmProtectionViolationSDPEntry Raised on class: sitesec.CpmProtViolSdpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the overall packet arrival rate limit at the SDP is violated.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower that acceptable in which case the configuration should be align with the traffic levels expected.		

Table 33-26 CpmProtectionViolationVdoSvcEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoSvcEntry (11188) Type: communications Package: sitesec.CpmProtectionViolationVdoSvcEntry Raised on class: sitesec.ServiceControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in VPLS Service.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 33-27 CpmProtectionViolationVdoVrtrClientEntry

Alarm	Attributes	Applicable major release
Name: CpmProtectionViolationVdoVrtrClientEntry (11189) Type: communications Package: sitesec.CpmProtectionViolationVdoVrtrClientEntry Raised on class: sitesec.RouterControlTrafficViolation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: denialOfService	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a per-source rate limit violation is detected for a client address of a Real-time Control Protocol (RTCP) control traffic in router context.		
Raising condition: ('Number of Rate Violations' NOT EQUAL '0L')		
Remedial action: A device in the network is sending traffic to the NE at a rate which is higher than expected. The source of the traffic must be identified and if the behavior is undesired then the device should be disabled. It is also possible that the threshold has been configured at a level which is lower than acceptable, in which case the configuration should be aligned with the expected traffic levels.		

Table 33-28 DDMAux1HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1HighAlarm (495) Type: thresholdAlarm Package: equipment.DDMAux1HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-29 DDMAux1HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1HighWarning (494) Type: thresholdAlarm Package: equipment.DDMAux1HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1HighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-29 DDMAux1HighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-30 DDMAux1LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux1LowAlarm (493) Type: thresholdAlarm Package: equipment.DDMAux1LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-31 DDMAux1LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux1LowWarning (492) Type: thresholdAlarm Package: equipment.DDMAux1LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux1LowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 1 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux1 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux1 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-32 DDMAux2HighAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2HighAlarm (499) Type: thresholdAlarm Package: equipment.DDMAux2HighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-33 DDMAux2HighWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2HighWarning (498) Type: thresholdAlarm Package: equipment.DDMAux2HighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2HighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-34 DDMAux2LowAlarm

Alarm	Attributes	Applicable major release
Name: DDMAux2LowAlarm (497) Type: thresholdAlarm Package: equipment.DDMAux2LowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-34 DDMAux2LowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-35 DDMAux2LowWarning

Alarm	Attributes	Applicable major release
Name: DDMAux2LowWarning (496) Type: communicatiothresholdAlarmnsAlarm Package: equipment.DDMAux2LowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aux2LowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the manufacturer-specific Auxiliary 2 of the XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Aux2 Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Aux2 Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-36 DDMRxOpticalPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighAlarm (491) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-37 DDMRxOpticalPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerHighWarning (490) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-38 DDMRxOpticalPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowAlarm (489) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the received optical power of an SFP or XFP reaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-39 DDMRxOpticalPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMRxOpticalPowerLowWarning (488) Type: thresholdAlarm Package: equipment.DDMRxOpticalPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rxOpticalPowerLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-39 DDMRxOpticalPowerLowWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the received optical power of an SFP or XFP approaches the minimum threshold value.		
Raising condition: ('failedThresholds'anyBit'Rx Optical Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Rx Optical Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-40 DDMSupplyVoltageHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighAlarm (479) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-41 DDMSupplyVoltageHighWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageHighWarning (478) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-42 DDMSupplyVoltageLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowAlarm (477) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-43 DDMSupplyVoltageLowWarning

Alarm	Attributes	Applicable major release
Name: DDMSupplyVoltageLowWarning (476) Type: thresholdAlarm Package: equipment.DDMSupplyVoltageLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: supplyVoltageLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the supply voltage of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Supply Voltage Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Supply Voltage Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-44 DDMTemperatureHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighAlarm (475) Type: thresholdAlarm Package: equipment.DDMTemperatureHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-44 DDMTemperatureHighAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-45 DDMTemperatureHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureHighWarning (474) Type: thresholdAlarm Package: equipment.DDMTemperatureHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-46 DDMTemperatureLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowAlarm (473) Type: thresholdAlarm Package: equipment.DDMTemperatureLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-47 DDMTemperatureLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTemperatureLowWarning (472) Type: thresholdAlarm Package: equipment.DDMTemperatureLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temperatureLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the temperature of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Temperature Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Temperature Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-48 DDMTxBiasCurrentHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighAlarm (483) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-49 DDMTxBiasCurrentHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentHighWarning (482) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-49 DDMTxBiasCurrentHighWarning (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-50 DDMTxBiasCurrentLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowAlarm (481) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-51 DDMTxBiasCurrentLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxBiasCurrentLowWarning (480) Type: thresholdAlarm Package: equipment.DDMTxBiasCurrentLowWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txBiasCurrentLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the transmit bias current of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Bias Current Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Bias Current Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-52 DDMTxOutputPowerHighAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighAlarm (487) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighAlarm Raised on class: equipment.AbstractDDM	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-53 DDMTxOutputPowerHighWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerHighWarning (486) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerHighWarning Raised on class: equipment.AbstractDDM	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerHighWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power High Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power High Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-54 DDMTxOutputPowerLowAlarm

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowAlarm (485) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowAlarm Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-54 DDMTxOutputPowerLowAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the output power of an SFP or XFP reaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Alarm')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Alarm'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-55 DDMTxOutputPowerLowWarning

Alarm	Attributes	Applicable major release
Name: DDMTxOutputPowerLowWarning (484) Type: thresholdAlarm Package: equipment.DDMTxOutputPowerLowWarning Raised on class: equipment.AbstractDDM	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txOutputPowerLowWarning	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the output power of an SFP or XFP approaches the maximum threshold value.		
Raising condition: ('failedThresholds'anyBit'Tx Output Power Low Warning')		
Clearing condition: NOT (('failedThresholds'anyBit'Tx Output Power Low Warning'))		
Remedial action: Informational. Check the environmental parameters of the transceiver and ensure that it is not faulty.		

Table 33-56 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 33-57 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 33-58 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 33-59 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-59 EquipmentFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 33-60 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 33-61 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		

Table 33-61 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 33-62 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 33-63 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 33-64 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 33-65 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 33-66 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 33-67 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 33-68 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 33-69 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 33-70 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 33-71 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 33-72 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 33-73 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 33-74 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 33-75 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 33-76 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 33-77 InstanceDown (srrp)

Alarm	Attributes	Applicable major release
Name: InstanceDown (284) Type: configurationAlarm Package: srrp.InstanceDown Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: instanceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that an SRRP instance is operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' EQUAL 'Initialize'))		
Clearing condition: (('Operational State' NOT EQUAL 'Initialize') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check the configuration of the instance		

Table 33-78 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 33-79 InterfaceDown (vpls)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: configurationAlarm Package: vpls.InterfaceDown Raised on class: vpls.L2ManagementInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an L2 management interface has an Operational State of Down, and the associated VPLS site has an Administrative State of Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 33-80 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 33-81 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 33-82 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-82 IsisInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 33-83 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 33-84 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		

Table 33-84 LabelProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 33-85 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 33-86 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 33-87 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 33-88 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 33-89 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-89 LdpTargetedPeerDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 33-90 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 33-91 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 33-92 LocalRncvOperDown

Alarm	Attributes	Applicable major release
Name: LocalRncvOperDown (521) Type: redundancyAlarm Package: multichassis.LocalRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: localRncvDisconnected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the local RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Local Operational State' NOT EQUAL 'Connected') AND ('Local Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Local Operational State' EQUAL 'Connected') OR ('Local Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 33-93 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 33-94 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 33-95 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 33-96 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 33-97 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 33-98 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-98 macMoveRateExceeded (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 33-99 MCLagDown (lag)

Alarm	Attributes	Applicable major release
Name: MCLagDown (394) Type: equipmentAlarm Package: lag.MCLagDown Raised on class: lag.MultiChassisLagSpecifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mcLagDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all ports in an MC LAG are operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 33-100 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		

Table 33-100 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 33-101 MissingLocalEntry

Alarm	Attributes	Applicable major release
Name: MissingLocalEntry (291) Type: configurationAlarm Package: l2fwd.MissingLocalEntry Raised on class: l2fwd.ServiceMacProtection	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Protected_Mac_Address_Not_Global	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a protected MAC address is not configured on all sites of a VPLS. This can occur if the protected MAC address is added or removed using a CLI.		
Raising condition: ('isEntryGlobal' EQUAL 'false')		
Clearing condition: ('isEntryGlobal' EQUAL 'true')		
Remedial action: Configure the 'Protected MAC Address' on all the VPLS sites.		

Table 33-102 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 33-103 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 33-104 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 33-105 MrpAttrTblSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MrpAttrTblSizeLimitReached (574) Type: resourceAlarm Package: l2fwd.MrpAttrTblSizeLimitReached Raised on class: l2fwd.SiteMrp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the number of MRP attribute table entries for a service site exceeds the high watermark specified by l2fwd.SiteMrp.mrpAttrTblHighWatermark. The alarm clears when the number of MRP attribute table entries for the site drops below the low watermark specified by l2fwd.SiteMrp.mrpAttrTblLowWatermark.		
Raising condition: (('MRP Attribute Count' >=" 'MRP Max Attributes') OR ('MRP Attribute Count' >= (('MRP Attribute-Table-High-Watermark' * 'MRP Max Attributes') / 100.0)))"		
Clearing condition: (('MRP Attribute Count' < 'MRP Max Attributes') AND (('MRP Attribute-Table-High-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))) AND (('MRP Attribute-Table-Low-Watermark' EQUAL '0') OR ('MRP Attribute Count' < (('MRP Attribute-Table-Low-Watermark' * 'MRP Max Attributes') / 100.0))))		
Remedial action: Informational		

Table 33-106 MsPwFecRetryExpired

Alarm	Attributes	Applicable major release
Name: MsPwFecRetryExpired (3694) Type: serviceAlarm Package: svt.MsPwFecRetryExpired Raised on class: svt.SpokeSdpFec	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecRetryExpired	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a trap is received because of retry expired. The alarm is cleared when the retry starts again.		
Raising condition: ('Retry Expired' EQUAL 'true')		
Clearing condition: ('Retry Expired' EQUAL 'false')		
Remedial action: May need to shutdown the multi-segment pseudo-wire provider edge to restart the retries.		

Table 33-107 MultiChassisRingDown

Alarm	Attributes	Applicable major release
Name: MultiChassisRingDown (520) Type: redundancyAlarm Package: multichassis.MultiChassisRingDown Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ringDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MC ring group Operational State is not in the Connected state. The alarm is cleared when the ring group enters the Connected state.		
Raising condition: ('Operational State' NOT EQUAL 'Connected')		
Clearing condition: ('Operational State' EQUAL 'Connected')		
Remedial action: Check if MC ring is admin down, MC Sync is operational up, In-Band Control Connection is up, ring node is up ...		

Table 33-108 MvrConfiguredFromVplsNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredFromVplsNotExist (219) Type: configurationAlarm Package: vpls.MvrConfiguredFromVplsNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredFromVplsNo-tExist	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MVR source is an MVR VPLS that does not exist. The alarm clears when the MVR VPLS is created.		
Raising condition: ('fromVplsExists' EQUAL 'false')		
Clearing condition: (('fromVplsExists' EQUAL 'true') OR ('fromVplsId' EQUAL '0L'))		
Remedial action: Create the missing MVR VPLS.		

Table 33-109 MvrConfiguredProxySapNotExist

Alarm	Attributes	Applicable major release
Name: MvrConfiguredProxySapNotExist (220) Type: configurationAlarm Package: vpls.MvrConfiguredProxySapNotExist Raised on classes: • vpls.L2AccessInterfaceMldMvrCfg • vpls.L2AccessInterfaceMvrCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MvrConfiguredProxySapNo-tExist	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configured MVR proxy SAP does not exist. The alarm clears when the proxy SAP is created.		
Raising condition: ('proxySapExists' EQUAL 'false')		
Clearing condition: ('proxySapExists' EQUAL 'true')		
Remedial action: Create the missing proxy SAP.		

Table 33-110 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 33-111 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-111 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 33-112 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 33-113 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 33-114 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 33-115 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 33-116 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 33-117 NoPeerMcRingFound

Alarm	Attributes	Applicable major release
Name: NoPeerMcRingFound (782) Type: configurationAlarm Package: multichassis.NoPeerMcRingFound Raised on class: multichassis.MultiChassisRing	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompleteConfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot find the peer MC ring.		
Raising condition: ('Peer Multi-Chassis Ring' EQUAL '\"\"')		
Clearing condition: ('Peer Multi-Chassis Ring' NOT EQUAL '\"\"')		
Remedial action: Configure the missing peered MC ring, or delete this one if it is not used.		

Table 33-118 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 33-119 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-119 OspfInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 33-120 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 33-121 P2MPLSPDown

Alarm	Attributes	Applicable major release
Name: P2MPLSPDown (4378) Type: pathAlarm Package: mpls.P2MPLSPDown Raised on class: mpls.P2MPDynamicLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: P2MPLSPDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the P2MP LSP Administrative State is Up and the Operational State is Down. The alarm clears when the P2MP LSP Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		

Table 33-121 P2MPLSPDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: The operational state of the P2MP LSP is down, despite the administrative state being up. Review the P2MP Primary Instance or S2LPath to make sure it was configured correctly and Administrative state is up. The physical port near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 33-122 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 33-123 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		

Table 33-123 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 33-124 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 33-125 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 33-126 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 33-127 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 33-128 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 33-129 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 33-130 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 33-131 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 33-132 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 33-133 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 33-134 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 33-135 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 33-136 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 33-137 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 33-138 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 33-139 RemoteRncvOperDown

Alarm	Attributes	Applicable major release
Name: RemoteRncvOperDown (522) Type: redundancyAlarm Package: multichassis.RemoteRncvOperDown Raised on class: multichassis.MultiChassisRingNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteRncvDisconnected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the remote RNCV Operational State of a ring node is other than Connected or NotTested, which means that the ring node is not connected to the local MC ring group. The alarm clears when the ring node enters the Connected or NotTested state.		
Raising condition: (('Remote Operational State' NOT EQUAL 'Connected') AND ('Remote Operational State' NOT EQUAL 'Not Tested'))		
Clearing condition: (('Remote Operational State' EQUAL 'Connected') OR ('Remote Operational State' EQUAL 'Not Tested'))		
Remedial action: Make sure that ring node is properly connected to MC ring group.		

Table 33-140 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 33-141 S2LPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: S2LPathBypassTunnelActive (777) Type: pathAlarm Package: mpls.S2LPathBypassTunnelActive Raised on class: mpls.S2LPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathReroutedToBypassTunnel	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the bypass tunnel in an S2L path becomes active. The alarm clears when the bypass tunnel is no longer active, for example, because a primary tunnel failure is resolved or a new path is established.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: Check what caused primary tunnel is down and fix it if possible.		

Table 33-142 S2LPathDown

Alarm	Attributes	Applicable major release
Name: S2LPathDown (778) Type: pathAlarm Package: mpls.S2LPathDown Raised on class: mpls.S2LPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: S2LPathDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the S2L path Administrative State is Up and the Operational State is not Up. The alarm clears when the S2L path Operational State changes to Up or the Administrative State changes to Down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 33-143 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 33-144 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 33-145 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 33-146 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 33-147 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 33-148 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 33-149 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 33-150 ShamLinkDown

Alarm	Attributes	Applicable major release
Name: ShamLinkDown (665) Type: ShamLinkAlarm Package: ospf.ShamLinkDown Raised on class: ospf.ShamLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ShamLinkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a sham link is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF sham link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 33-151 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 33-152 SpbAdjacencyDown

Alarm	Attributes	Applicable major release
Name: SpbAdjacencyDown (4392) Type: adjacencyAlarm Package: spb.SpbAdjacencyDown Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L'))		
Clearing condition: (('Adjacency Count' > '0L'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 33-153 SpbInterfaceDown

Alarm	Attributes	Applicable major release
Name: SpbInterfaceDown (4393) Type: ProtocolAlarm Package: spb.SpbInterfaceDown Raised on class: spb.AbstractInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an SPB IS-IS interface has an Operational State other than Up.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 33-154 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-154 SpbSiteDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 33-155 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 33-156 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 33-156 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 33-157 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 33-158 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 33-159 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 33-160 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 33-161 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-161 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 33-162 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		

Table 33-162 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 33-163 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 33-164 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 33-165 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 33-166 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 33-167 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-167 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 33-168 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 33-169 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 33-170 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 33-171 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 33-172 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0

Table 33-172 UplinkPartiallyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 33-173 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 33-174 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 33-174 VirtualLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 33-175 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 33-176 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 2.1 • 3.0 • 3.1 • 3.2 • 4.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

34 DSC

34.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 34-1 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 34-2 AtcaCardTemperatureLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardTemperatureLowerThresholdAlarm (3710) Type: equipmentAlarm Package: equipment. AtcaCardTemperatureLowerThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardTemperatureLow	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the ATCA card temperature has decreased below any of the lower thresholds.		
Raising condition: ('Temperature Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Informational - no corrective action required.		

Table 34-3 AtcaCardTemperatureUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardTemperatureUpperThresholdAlarm (3711) Type: equipmentAlarm Package: equipment.AtcaCardTemperatureUpperThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardTemperatureHigh	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the ATCA card temperature has increased beyond any of the upper thresholds.		
Raising condition: ('Temperature Threshold State' EQUAL 'Upper Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor the blade. If the condition persists, replace the blade. If the condition applies to more than one blade, verify the performance of the site cooling system.		

Table 34-4 AtcaCardVoltageLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardVoltageLowerThresholdAlarm (3712) Type: equipmentAlarm Package: equipment.AtcaCardVoltageLowerThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardVoltageLow	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the ATCA card voltage level has decreased below any of the lower thresholds.		
Raising condition: ('Voltage Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the blade is in the active state, it should be replaced.		

Table 34-5 AtcaCardVoltageUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: AtcaCardVoltageUpperThresholdAlarm (3713) Type: equipmentAlarm Package: equipment.AtcaCardVoltageUpperThresholdAlarm Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AtcaCardVoltageHigh	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the ATCA card voltage level has increased beyond any of the upper thresholds.		
Raising condition: ('Voltage Threshold State' EQUAL 'Upper Critical')		

Table 34-5 AtcaCardVoltageUpperThresholdAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the blade is in the active state, it should be replaced.		

Table 34-6 AtcaFanFailure

Alarm	Attributes	Applicable major release
Name: AtcaFanFailure (1124) Type: equipmentAlarm Package: equipment.AtcaFanFailure Raised on class: equipment.Fan	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled') OR ('operationalState' EQUAL 'Down'))		
Clearing condition: (('operationalState' EQUAL 'Enabled') OR ('operationalState' EQUAL 'Up'))		
Remedial action: This alarm is raised if the fan speed falls below 500 rpm. If the alarm persists, replace the appropriate (upper or lower) fan tray.		

Table 34-7 AtcaPowerSupplyFailure

Alarm	Attributes	Applicable major release
Name: AtcaPowerSupplyFailure (1125) Type: equipmentAlarm Package: equipment.AtcaPowerSupplyFailure Raised on class: equipment.PowerSupply	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the associated power supply is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled'))		
Clearing condition: ('operationalState' EQUAL 'Enabled')		
Remedial action: Check the status of the site power supply.		

Table 34-8 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 34-9 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 34-10 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 34-10 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 34-11 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 34-12 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		

Table 34-12 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 34-13 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 34-14 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 34-15 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 34-16 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 34-17 DiameterMonitoredDestinationOverloaded

Alarm	Attributes	Applicable major release
Name: DiameterMonitoredDestinationOverloaded (7959) Type: EpcAlarm Package: lte. DiameterMonitoredDestinationOverloaded Raised on class: lte.DscDiameterMonDestination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DscOverloadStateChange	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 34-17 DiameterMonitoredDestinationOverloaded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the overload state of a monitored destination changes from normal.		
Raising condition: (('Overload State' EQUAL 'Critical') OR ('Overload State' EQUAL 'Resource Critical'))		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: The overload state of a monitored destination has changed from normal. Verify the threshold limit of the destination.		

Table 34-18 DiskTemperatureLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: DiskTemperatureLowerThresholdAlarm (3716) Type: equipmentAlarm Package: equipment. DiskTemperatureLowerThresholdAlarm Raised on class: equipment.Disk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiskTemperatureLow	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the disk temperature decreases below a lower threshold.		
Raising condition: ('Temperature Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Informational - no corrective action required.		

Table 34-19 DiskTemperatureUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: DiskTemperatureUpperThresholdAlarm (3717) Type: equipmentAlarm Package: equipment. DiskTemperatureUpperThresholdAlarm Raised on class: equipment.Disk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiskTemperatureHigh	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the disk temperature increases above an upper threshold.		
Raising condition: ('Temperature Threshold State' EQUAL 'Upper Critical')		
Clearing condition: ('Temperature Threshold State' EQUAL 'Unspecified')		
Remedial action: Check the site cooling mechanism. If the alarm persists, replace the disk.		

Table 34-20 DiskVoltageLowerThresholdAlarm

Alarm	Attributes	Applicable major release
Name: DiskVoltageLowerThresholdAlarm (3718) Type: equipmentAlarm Package: equipment. DiskVoltageLowerThresholdAlarm Raised on class: equipment.Disk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiskVoltageLow	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the disk voltage level decreases below a lower threshold.		
Raising condition: ('Voltage Threshold State' EQUAL 'Lower Critical')		
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the disk is in the active state, it should be replaced.		

Table 34-21 DiskVoltageUpperThresholdAlarm

Alarm	Attributes	Applicable major release
Name: DiskVoltageUpperThresholdAlarm (3719) Type: equipmentAlarm Package: equipment. DiskVoltageUpperThresholdAlarm Raised on class: equipment.Disk	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DiskVoltageHigh	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the disk voltage level increases above an upper threshold.		
Raising condition: ('Voltage Threshold State' EQUAL 'Upper Critical')		
Clearing condition: ('Voltage Threshold State' EQUAL 'Unspecified')		
Remedial action: Monitor. If the alarm persists and the disk is in the active state, it should be replaced.		

Table 34-22 DscExtSystemOperStateDown

Alarm	Attributes	Applicable major release
Name: DscExtSystemOperStateDown (7960) Type: EpcAlarm Package: lte.DscExtSystemOperStateDown Raised on class: lte.DscExtSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DscExtSystemOperStateDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the operational state of an external system is down.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		

Table 34-22 DscExtSystemOperStateDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of an external system is down (not connected). Verify its connection.		

Table 34-23 DscGeoRedundancyFailure

Alarm	Attributes	Applicable major release
Name: DscGeoRedundancyFailure (8153) Type: EpcAlarm Package: lte.DscGeoRedundancyFailure Raised on class: lte.ServiceContainer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfRedundancy	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a DSC loses Geo Redundancy.		
Raising condition: (('Geo-Redundancy' EQUAL 'Standalone'))		
Clearing condition: (('Geo-Redundancy' EQUAL 'Redundant'))		
Remedial action: Check the operational state of both geo-mates. If failed, the operator must recover both geo-mates. If geo-mates are operational, the root cause must be a failure in the WAN link used for geo-redundancy, which must be corrected.		

Table 34-24 DscPlatformLicenseKeyExpiredAlarm

Alarm	Attributes	Applicable major release
Name: DscPlatformLicenseKeyExpiredAlarm (1133) Type: EpcAlarm Package: lte.DscPlatformLicenseKeyExpiredAlarm Raised on class: lte. DynamicServicesControllerInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DscPlatformLicenseKeyExpired	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the DSC platform license key is expired.		
Remedial action: Contact your Nokia support representative to obtain new DSC license key		

Table 34-25 DscPlatformLicenseKeyExpiringAlarm

Alarm	Attributes	Applicable major release
Name: DscPlatformLicenseKeyExpiringAlarm (1134) Type: EpcAlarm Package: lte.DscPlatformLicenseKeyExpiringAlarm Raised on class: lte. DynamicServicesControllerInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DscPlatformLicenseKeyExpiring	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 34-25 DscPlatformLicenseKeyExpiringAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the DSC platform license key is expiring.		
Remedial action: Contact your Nokia support representative to obtain new DSC license key		

Table 34-26 DscPlatformLicenseKeyHighWaterAlarm

Alarm	Attributes	Applicable major release
Name: DscPlatformLicenseKeyHighWaterAlarm (1135) Type: EpcAlarm Package: lte.DscPlatformLicenseKeyHighWaterAlarm Raised on class: lte.DynamicServicesControllerInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DscPlatformLicenseKeyHighWaterMarkCrossed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the DSC license key crosses the high watermark for a specified threshold.		
Remedial action: Contact your Nokia support representative to obtain new DSC license key		

Table 34-27 DscPlatformLicenseKeyLowWaterAlarm

Alarm	Attributes	Applicable major release
Name: DscPlatformLicenseKeyLowWaterAlarm (1136) Type: EpcAlarm Package: lte.DscPlatformLicenseKeyLowWaterAlarm Raised on class: lte.DynamicServicesControllerInstance	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DscPlatformLicenseKeyLowWaterMarkCrossed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the DSC license key crosses the low watermark for a specified threshold.		
Remedial action: Contact your Nokia support representative to obtain new DSC license key		

Table 34-28 DscPlatformLicenseKeyThresholdReachedAlarm

Alarm	Attributes	Applicable major release
Name: DscPlatformLicenseKeyThresholdReachedAlarm (1137) Type: EpcAlarm Package: lte.DscPlatformLicenseKeyThresholdReachedAlarm Raised on class: lte.DynamicServicesControllerInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DscPlatformLicenseKeyThresholdReached	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the DSC license key reaches a specified threshold.		

Table 34-28 DscPlatformLicenseKeyThresholdReachedAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: NContact your Nokia support representative to obtain new DSC license key		

Table 34-29 DscServiceContainerDown

Alarm	Attributes	Applicable major release
Name: DscServiceContainerDown (845) Type: EpcAlarm Package: lte.DscServiceContainerDown Raised on class: lte.ServiceContainer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DscServiceDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a DSC service container is down.		
Raising condition: (('Operational State' EQUAL 'Disabled'))		
Clearing condition: (('Operational State' EQUAL 'Enabled'))		
Remedial action: Investigate /opt/tpa/logs/RACServer.log on the CSB to determine cause of service container failure.		

Table 34-30 DscServiceDown

Alarm	Attributes	Applicable major release
Name: DscServiceDown (846) Type: EpcAlarm Package: lte.DscServiceDown Raised on class: lte. AbstractDynamicServicesControllerMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DscServiceDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a DSC service member is down.		
Raising condition: (('Operational State' EQUAL 'Disabled'))		
Clearing condition: (('Operational State' EQUAL 'Enabled'))		
Remedial action: Investigate /opt/tpa/logs/RACServer.log on the CSB to determine cause of service failure.		

Table 34-31 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 34-32 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 34-33 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		

Table 34-33 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 34-34 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 34-35 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 34-36 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 34-37 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 34-38 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		

Table 34-38 FanFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 34-39 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 34-40 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 34-41 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 34-42 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 34-43 NodeRebooted

Alarm	Attributes	Applicable major release
Name: NodeRebooted (32) Type: equipmentAlarm Package: netw.NodeRebooted Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeReboot	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects an NE reboot based on the latest NE sysUpTime value.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 34-44 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 34-45 OverloadedCard

Alarm	Attributes	Applicable major release
Name: OverloadedCard (2941) Type: cardAlarm Package: equipment.OverloadedCard Raised on class: equipment.AtcaCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: overloadedCard	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an ATCA card becomes overloaded.		
Raising condition: (('Overload State' EQUAL 'Critical') OR ('Overload State' EQUAL 'Resource Critical'))		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Investigate /opt/tpa/logs/RACServer.log on the CSB to determine cause of system overload.		

Table 34-46 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		

Table 34-46 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 34-47 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 34-48 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 34-49 PowerSupplyInputFeedDownAlarm

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDownAlarm (5154) Type: equipmentAlarm Package: equipment. PowerSupplyInputFeedDownAlarm Raised on class: equipment.PowerSupply	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('Input Feed Status' EQUAL 'Input A Down') OR ('Input Feed Status' EQUAL 'Input B Down') OR (('Input Feed Status'allBits'Input A Down') AND ('Input Feed Status'allBits'Input B Down')))		
Clearing condition: ('Input Feed Status' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power		

Table 34-50 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 34-51 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 34-51 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 34-52 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 34-53 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 34-54 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 34-55 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 34-56 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.0 • 7.0 • 8.0 • 9.0

Table 34-56 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 34-57 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 34-58 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 34-59 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.0 • 7.0 • 8.0 • 9.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

35 FlexiPacket MultiRadio

35.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 35-1 ACCMConfigError

Alarm	Attributes	Applicable major release
Name: ACCMConfigError (11243) Type: processingErrorAlarm Package: dw.ACCMConfigError Raised on class: dw.DwAlarmedObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: The content of a received A-CCM message is not coherent with the configuration.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-2 ACCMLoss

Alarm	Attributes	Applicable major release
Name: ACCMLoss (11244) Type: processingErrorAlarm Package: dw.ACCMLoss Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: ODU does not receive a valid CCM in the relevant MA.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-3 AccountLogFilledFirstThreshold

Alarm	Attributes	Applicable major release
Name: AccountLogFilledFirstThreshold (11470) Type: processingErrorAlarm Package: netw.AccountLogFilledFirstThreshold Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when the first threshold on account log is crossed.		

Table 35-3 AccountLogFilledFirstThreshold (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-4 AccountLogFilledSecondThreshold

Alarm	Attributes	Applicable major release
Name: AccountLogFilledSecondThreshold (11471) Type: processingErrorAlarm Package: netw.AccountLogFilledSecondThreshold Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when the second threshold on account log is crossed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-5 AirLoss

Alarm	Attributes	Applicable major release
Name: AirLoss (11280) Type: processingErrorAlarm Package: equipment.AirLoss Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: Triggered when the RX constellation is not locked. The trigger depends on the RX Modulation in use (the airLoss threshold depends on modulation format). Action: Check the RF quality including the received power and received S/MSE value.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-6 ATPCAutoDisabled

Alarm	Attributes	Applicable major release
Name: ATPCAutoDisabled (11469) Type: processingErrorAlarm Package: netw.ATPCAutoDisabled Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: Transmit power stays at Pmax for at least the continuative period of time defined by ATPC Cfg Intervention Timer.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-7 AutonegotiationConfigurationError

Alarm	Attributes	Applicable major release
Name: AutonegotiationConfigurationError (11281) Type: processingErrorAlarm Package: equipment. AutonegotiationConfigurationError Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: Auto-negotiation capabilities do not match the Synch settings. Possible causes: misconfiguration of the equipment.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-8 CollocatedMEPStateDown

Alarm	Attributes	Applicable major release
Name: CollocatedMEPStateDown (11246) Type: processingErrorAlarm Package: dw.CollocatedMEPStateDown Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: The operational state of the collocated MEP State machine is down.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-9 ConfigurationError

Alarm	Attributes	Applicable major release
Name: ConfigurationError (11473) Type: processingErrorAlarm Package: netw.ConfigurationError Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: The MultiRadio ODU has received SSM carrying a DNU code from at least one synchronization interface. Possible causes: misconfiguration of the peer equipment.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-10 ConfigurationNotSupported

Alarm	Attributes	Applicable major release
Name: ConfigurationNotSupported (11474) Type: processingErrorAlarm Package: netw.ConfigurationNotSupported Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: The current configuration such as system type vs profile is not supported		

Table 35-10 ConfigurationNotSupported (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-11 ECCMConfigError

Alarm	Attributes	Applicable major release
Name: ECCMConfigError (11247) Type: processingErrorAlarm Package: dw.ECCMConfigError Raised on class: dw.DwAlarmedObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: The content of a received E-CCM message is not coherent with the configuration;Action: change the configuration of one MultiRadio to have the same configuration of the second MultiRadio.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-12 ECCMLoss

Alarm	Attributes	Applicable major release
Name: ECCMLoss (11248) Type: processingErrorAlarm Package: dw.ECCMLoss Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: E-CCMs messages are exchanged between the IDU and the ODU; ODU does not receive a valid CCM in the relevant MA. Only if System type is protected.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-13 FpmrSelfTestFailure

Alarm	Attributes	Applicable major release
Name: FpmrSelfTestFailure (11476) Type: processingErrorAlarm Package: netw.FpmrSelfTestFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: Self-test output procedure failed.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-14 FpmrSystemFailure

Alarm	Attributes	Applicable major release
Name: FpmrSystemFailure (11477) Type: equipmentAlarm Package: netw.FpmrSystemFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: The MultiRadio is out of service the RF Transmitter is squelched. MultiRadio must be replaced. Action: Reset the Controller. If the alarm is still active replace MultiRadio.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-15 FragmentationError

Alarm	Attributes	Applicable major release
Name: FragmentationError (11478) Type: processingErrorAlarm Package: netw.FragmentationError Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarms is raised when the field fpmrQosfgFragmentationEn is successfully set to enabled but the fragmentation is not done at the side because of:1. The SVR on the remote side ODU is less than 2.52. Locally the number of configured strict priority queues is 0.The alarm is cleared when the fragmentation is disabled or when the conditions above have been removed.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-16 HighBER (netw)

Alarm	Attributes	Applicable major release
Name: HighBER (682) Type: processingErrorAlarm Package: netw.HighBER Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: Local ODU detects an High BER (near the threshold of the Data Loss).		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-17 HSBYConfigurationError

Alarm	Attributes	Applicable major release
Name: HSBYConfigurationError (11479) Type: processingErrorAlarm Package: netw.HSBYConfigurationError Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A

Table 35-17 HSBYConfigurationError (continued)

Alarm	Attributes	Applicable major release
Description: ODU received 9 consecutive P-CCM (OK ON) (P-CCM(OK OFF)) when in ON (OFF) state.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-18 HybridPacketMismatch

Alarm	Attributes	Applicable major release
Name: HybridPacketMismatch (11480) Type: processingErrorAlarm Package: netw.HybridPacketMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: There is a hybrid/packet mismatch between STBY and active software.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-19 LOF

Alarm	Attributes	Applicable major release
Name: LOF (11292) Type: processingErrorAlarm Package: equipment.LOF Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CableInerfaceError	Release: • N/A
Description: There is a LOF at IDU-ODU cable frame level.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-20 ManualOperationOn

Alarm	Attributes	Applicable major release
Name: ManualOperationOn (11481) Type: processingErrorAlarm Package: netw.ManualOperationOn Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is related to Test/Manual Operation. It is raised when at least one test configuration is active.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-21 MauStatusDown

Alarm	Attributes	Applicable major release
Name: MauStatusDown (11293) Type: processingErrorAlarm Package: equipment.MauStatusDown Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This object identifies Media Available state of the MAU interface.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-22 ModemSignalUnderThreshold

Alarm	Attributes	Applicable major release
Name: ModemSignalUnderThreshold (11482) Type: equipmentAlarm Package: netw.ModemSignalUnderThreshold Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: Triggered when the signal level after the ADC in the Modem section is below a fixed threshold.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-23 MultipleMatchInPacketIdentification

Alarm	Attributes	Applicable major release
Name: MultipleMatchInPacketIdentification (11484) Type: processingErrorAlarm Package: netw.MultipleMatchInPacketIdentification Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: When raised, at least one packet has not been compressed because of muiltiple rule matching.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-24 NotHybridInterface

Alarm	Attributes	Applicable major release
Name: NotHybridInterface (11486) Type: processingErrorAlarm Package: netw.NotHybridInterface Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CableInerfaceError	Release: • N/A
Description: The IDU is not properly working for this application.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-25 OAM_RDI

Alarm	Attributes	Applicable major release
Name: OAM_RDI (11253) Type: processingErrorAlarm Package: dw.OAM_RDI Raised on class: dw.DwAlarmedObject	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OAMError	Release: • N/A
Description: State of the RDI bit in the last received CCM (true for RDI="1) or false if none has been received. CRITICAL if System type is(1+0). Most probable cause: Connection problem with Microwave Hub (MultiRadio receives messages from Microwave Hub but Hub does not receives messages from the MultiRadio). Action: Reset the Controller. If the alarm is still active check the connectivity between MultiRadio and Hub."		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-26 ODUContinuityCheckLoss

Alarm	Attributes	Applicable major release
Name: ODUContinuityCheckLoss (11254) Type: processingErrorAlarm Package: dw.ODUContinuityCheckLoss Raised on class: dw.DwAlarmedObject	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OAMError	Release: • N/A
Description: ODU does not receive a valid CCM in the relevant MA. IDU is not properly set and it doesn't send CCM messages to ODU or IDU-ODU connectivity is compromised. Action: Check IDU settings or check IDU-ODU connectivity.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-27 ODUODUPortFailure

Alarm	Attributes	Applicable major release
Name: ODUODUPortFailure (11809) Type: processingErrorAlarm Package: equipment.ODUODUPortFailure Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: The ODU to ODU connection is lost. Action: Check the cable. If the cable is OK check in the Alarm list the active alarm.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-28 ODUSynchMissingSSM

Alarm	Attributes	Applicable major release
Name: ODUSynchMissingSSM (11488) Type: processingErrorAlarm Package: netw.ODUSynchMissingSSM Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A

Table 35-28 ODUSynchMissingSSM (continued)

Alarm	Attributes	Applicable major release
Description: The MultiRadio ODU doesn't receive SSM messages from the selected synchronization interface. Possible causes: misconfiguration of the peer equipment. Action: Check the synchronization network configuration.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-29 PacketDischarging

Alarm	Attributes	Applicable major release
Name: PacketDischarging (11298) Type: processingErrorAlarm Package: equipment.PacketDischarging Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CableInerfaceError	Release: • N/A
Description: FPGA is discharging packets from IDU.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-30 PCCMConfigError

Alarm	Attributes	Applicable major release
Name: PCCMConfigError (11255) Type: processingErrorAlarm Package: dw.PCCMConfigError Raised on class: dw.DwAlarmedObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: The content of a received P-CCM message is not coherent with the configuration; Action: change the configuration of one MultiRadio to have the same configuration of the second MultiRadio.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-31 PCCMLoss

Alarm	Attributes	Applicable major release
Name: PCCMLoss (11256) Type: processingErrorAlarm Package: dw.PCCMLoss Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: P-CCM messages are exchanged between the two ODUs belonging to the same MA; ODU does not receive a valid CCM in the relevant MA.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-32 PortDown

Alarm	Attributes	Applicable major release
Name: PortDown (11299) Type: communicationsAlarm Package: equipment.PortDown Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • N/A
Description: This alarm is raised when the Operational State of Port goes down when the Admin State is up.		
Remedial action: Please refer to Troubleshooting Guide for remedial action.		

Table 35-33 PowerSupplyFailure (netw)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: netw.PowerSupplyFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: Failure in the internal DC/DC converter.MultiRadio must be replaced. Action: Check the voltage of the station battery. If OK replace MultiRadio.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-34 ProtectionModeMismatch

Alarm	Attributes	Applicable major release
Name: ProtectionModeMismatch (11490) Type: processingErrorAlarm Package: netw.ProtectionModeMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: Wrong configuration of Protection Mode.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-35 RadioFrameLoss

Alarm	Attributes	Applicable major release
Name: RadioFrameLoss (11305) Type: processingErrorAlarm Package: equipment.RadioFrameLoss Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A

Table 35-35 RadioFrameLoss (continued)

Alarm	Attributes	Applicable major release
Description: The MultiRadio ODU detects an RxFail in the RX function. It is triggered by the Loss of the synchronization with the frame preamble; it is independent from the data modulation. Most probable causes and actions: (a) The radio path is down cannot receive signal from remote ODU. Clean the radio path or check the remote ODU TX power. (b) Configuration problem the frequency is different from remote ODU. Align ODU frequency configuration for both sides. (c) Remote ODU radio port squelch. Set remote ODU radio port up.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-36 RDIReceivedInLastACCM

Alarm	Attributes	Applicable major release
Name: RDIReceivedInLastACCM (11259) Type: processingErrorAlarm Package: dw.RDIReceivedInLastACCM Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OAMError	Release: • N/A
Description: State of the RDI bit in the last received A-CCM (true for RDI="1) or false if none has been received."		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-37 RDIReceivedInLastECCM

Alarm	Attributes	Applicable major release
Name: RDIReceivedInLastECCM (11260) Type: processingErrorAlarm Package: dw.RDIReceivedInLastECCM Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OAMError	Release: • N/A
Description: State of the RDI bit in the last received E-CCM (true for RDI="1) or false if none has been received."		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-38 RDIReceivedInLastPCCM

Alarm	Attributes	Applicable major release
Name: RDIReceivedInLastPCCM (11261) Type: processingErrorAlarm Package: dw.RDIReceivedInLastPCCM Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OAMError	Release: • N/A
Description: State of the RDI bit in the last received P-CCM (true for RDI="1) or false if none has been received."		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-39 RolePriorityMismatch

Alarm	Attributes	Applicable major release
Name: RolePriorityMismatch (11492) Type: processingErrorAlarm Package: netw.RolePriorityMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: Wrong configuration of Role/Priority.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-40 RxTimerReferenceMissing

Alarm	Attributes	Applicable major release
Name: RxTimerReferenceMissing (11493) Type: processingErrorAlarm Package: netw.RxTimerReferenceMissing Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CableInerfaceError	Release: • N/A
Description: Rx Timer Reference is missing.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-41 ScheduledActionFailure

Alarm	Attributes	Applicable major release
Name: ScheduledActionFailure (11272) Type: processingErrorAlarm Package: dw.ScheduledActionFailure Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is generated whenever a scheduled operation has failed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-42 SoftwareSwitchNotAllowed

Alarm	Attributes	Applicable major release
Name: SoftwareSwitchNotAllowed (11495) Type: processingErrorAlarm Package: netw.SoftwareSwitchNotAllowed Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when Switching action is initiated when not allowed. When any component Standby FW version is not compatible with the HW version, the switch command can not be executed. A new software must be downloaded.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-43 SwHwMismatch

Alarm	Attributes	Applicable major release
Name: SwHwMismatch (11497) Type: equipmentAlarm Package: netw.SwHwMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised to indicate Software/Firmware and Hardware mismatch. This occurs when the loaded SW and FW is not compatible with HW.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-44 SynchAllSourcesDown

Alarm	Attributes	Applicable major release
Name: SynchAllSourcesDown (11498) Type: communicationsAlarm Package: netw.SynchAllSourcesDown Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: This alarm is raised when a physical layer problem in all the configured synchronization interfaces is detected. Possible causes for IDU: (a) LinkState="DOWN has been detected in the Ethernet interface selected as synchronization interface. (b) LOS has been detected in the E1 interface selected as synchronization interface. As a consequent action the equipment will go to holdover state. The alarm is masked when the system is in Internal Synchronization Mode. Possible causes for ODU: The MultiRadio ODU has detected a physical layer problem in all the configured synchronization interfaces. As a consequent action the equipment will go to holdover state. Action: Check the synchronization sources."		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-45 SynchOneSourceDown (netw)

Alarm	Attributes	Applicable major release
Name: SynchOneSourceDown (11277) Type: processingErrorAlarm Package: netw.SynchOneSourceDown Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: Multiple synchronization interfaces are configured and when detecting a physical layer problem in at least one of the synchronization interfaces. Action: Check the synchronization sources.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-46 SystemTypeMismatch

Alarm	Attributes	Applicable major release
Name: SystemTypeMismatch (11501) Type: processingErrorAlarm Package: netw.SystemTypeMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: The Collocated ODU has a different system type configuration. An ODU configured as DD in either Trunk or Chain role reveals that the other ODU connected on the ODUODU interface is configured: (a) In a different system type (by means of the A-CCM protocol) (b) With the same system role (by means of the A-CCM protocol).		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-47 SystemTypeMismatchInPairedODUGroup

Alarm	Attributes	Applicable major release
Name: SystemTypeMismatchInPairedODUGroup (11502) Type: processingErrorAlarm Package: netw. SystemTypeMismatchInPairedODUGroup Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: This alarm can be raised only if system type is 2+2 XPIC. It represents wrong configuration in system type in paired ODU group.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-48 TimeServerMissing

Alarm	Attributes	Applicable major release
Name: TimeServerMissing (11503) Type: communicationsAlarm Package: netw.TimeServerMissing Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: This alarm is raised when the Time Server is missing. Cleared when time server answers. Action: Check the cable.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 35-49 TrapOutOfSequence

Alarm	Attributes	Applicable major release
Name: TrapOutOfSequence (11504) Type: equipmentAlarm Package: netw.TrapOutOfSequence Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingTrap	Release: • N/A
Description: This alarm is raised when SAM receives a trap that is out of sequence. This indicates some trap(s) sent from node did not reach SAM. When SAM receives an alarm that is out of sequence, SAM automaticlally synchronizes the Active Alarms on the Node and state information (Admin and Oper states) on all Ports. However, if any traps related to equipment configuration and service do not reach SAM, Full Node Sync needs to be manually triggered in order to synchronize Node with SAM.		
Remedial action: Please trigger Full Node Synchronization on the Node.		

Table 35-50 TxPowerAlarm

Alarm	Attributes	Applicable major release
Name: TxPowerAlarm (11505) Type: equipmentAlarm Package: netw.TxPowerAlarm Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: TX power 3 dB (or more) lower than requested TX power at the output of the RF Transmitter. FPR must be replaced. Action: FPR must be replaced.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

Table 35-51 WrongRoleOrPriorityInPairedODUGroup

Alarm	Attributes	Applicable major release
Name: WrongRoleOrPriorityInPairedODUGroup (11510) Type: processingErrorAlarm Package: netw. WrongRoleOrPriorityInPairedODUGroup Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionError	Release: • N/A
Description: This alarm can be raised only if system type is 2+2 XPIC. It represents wrong configuration in Role/Priority in paired ODU group.		
Remedial action: Please refer to FPMR Troubleshooting Guide for remedial action.		

36 Generic NE

36.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 36-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 1.0.0
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 36-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 1.0.0
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 36-3 adjacencyDown

Alarm	Attributes	Applicable major release
Name: adjacencyDown (11462) Type: communicationsAlarm Package: mpr.adjacencyDown Raised on class: mpr.BackhaulAdjacency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: adjacencyDown	Release: • 1.0.0
Description: The alarm is raised when the Operational State of a adjacency is Down, for example, because of one of the following conditions: The Operational State of local port pointer is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: NE Alarms causing operState down must not exist on the selected adjancency.		

Table 36-4 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 1.0.0
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 36-5 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 1.0.0
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 36-6 AncillaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: AncillaryPathLimitReached (459) Type: resourceAlarm Package: equipment.AncillaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 1.0.0
Description: The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached.		
Raising condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' >=" (1000 * 'Ancillary Path Limit Override')))"		
Clearing condition: (('Ancillary Path Limit Override' > '0') AND ('Ancillary Path In use' < (1000 * 'Ancillary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management ancillary path bandwidth limit is reached. This can be remedied by modifying the ancillary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the ancillary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 36-7 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 1.0.0
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 36-8 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 1.0.0
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		

Table 36-8 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 36-9 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 1.0.0
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 36-10 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 36-11 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 1.0.0

Table 36-11 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 36-12 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 36-13 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 1.0.0
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		

Table 36-13 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 36-14 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 1.0.0
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 36-15 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 1.0.0
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 36-16 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 36-17 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 36-18 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 36-18 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 36-19 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 1.0.0
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 36-20 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 1.0.0
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 36-21 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 36-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 36-23 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 1.0.0
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 36-24 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 36-25 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 1.0.0
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 36-26 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 1.0.0
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		

Table 36-26 ForwardingTableSizeLimitReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational		

Table 36-27 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 1.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 36-28 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 1.0.0
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 36-29 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 1.0.0
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		

Table 36-29 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 36-30 GenericInterfaceLinkDown

Alarm	Attributes	Applicable major release
Name: GenericInterfaceLinkDown (403) Type: equipmentAlarm Package: genericne.GenericInterfaceLinkDown Raised on class: genericne.GenericNeInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM detects a communication link failure on a GNE interface. The alarm clears when the link returns to service.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: The Operational State of the generic NE interface is down. The physical port (near end or far end) may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 36-31 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 36-32 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 1.0.0
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 36-33 inSufficientBandwidth

Alarm	Attributes	Applicable major release
Name: inSufficientBandwidth (11464) Type: serviceAlarm Package: mpr.inSufficientBandwidth Raised on class: mpr.BackhaulAdjacency	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inSufficientBandwidth	Release: • 1.0.0
Description: The alarm is raised when a deployed adjacency doesnt have sufficent bandwidth.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('isBandwidthExceeded' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') OR ('isBandwidthExceeded' EQUAL 'false'))		
Remedial action: Increase the bandwidth.		

Table 36-34 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 1.0.0
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 36-35 IsisAdjacencyDown

Alarm	Attributes	Applicable major release
Name: IsisAdjacencyDown (153) Type: adjacencyAlarm Package: isis.IsisAdjacencyDown Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsisInterfaceDown	Release: • 1.0.0
Description: The alarm is raised when an IS-IS interface has no adjacencies, for example, because the IS-IS protocol on the remote site is down.		
Raising condition: (('Adjacency Count' EQUAL '0L') AND ('interfaceClass' NOT EQUAL 'System') AND ('Passive' NOT EQUAL 'True'))		
Clearing condition: (('Adjacency Count' > '0L') OR ('Passive' EQUAL 'True'))		
Remedial action: Check remote site to see if corresponding IS-IS interface is configured and admin up.		

Table 36-36 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 36-37 IsisInterfaceDown

Alarm	Attributes	Applicable major release
Name: IsisInterfaceDown (301) Type: ProtocolAlarm Package: isis.IsisInterfaceDown Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an IS-IS interface has an Operational State other than Up.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: Check if underlying port is down, or associated network interface is down.		

Table 36-38 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 36-39 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 1.0.0
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 36-40 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 1.0.0
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		

Table 36-40 LagPortAddFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 36-41 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 36-42 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 36-43 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 1.0.0
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		

Table 36-43 LicensedLimitExceeded (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 36-44 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 1.0.0
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 36-45 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 1.0.0
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 36-46 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 1.0.0
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 36-47 LspPathBypassTunnelActive

Alarm	Attributes	Applicable major release
Name: LspPathBypassTunnelActive (264) Type: pathAlarm Package: mpls.LspPathBypassTunnelActive Raised on class: mpls.LspPath	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathReroutedToBypass-Tunnel	Release: • 1.0.0
Description: The alarm is raised when an LSP primary path is rerouted to the bypass tunnel. The alarm clears when the primary path returns to the original tunnel and the actual hop returns to the primary path.		
Raising condition: ('Bypass Tunnel Active' EQUAL 'true')		
Clearing condition: ('Bypass Tunnel Active' EQUAL 'false')		
Remedial action: There is a problem with the original path, check what is the problem and fix it if possible.		

Table 36-48 LspPathDown

Alarm	Attributes	Applicable major release
Name: LspPathDown (26) Type: pathAlarm Package: mpls.LspPathDown Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspPathDown	Release: • 1.0.0
Description: The alarm is raised when an LSP path is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up') AND ('Type' EQUAL 'Standby'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up') OR ('Type' EQUAL 'Secondary'))		
Remedial action: Check the failure code and update accordingly, e.g. whether MPLS/RSVP interfaces, OSPF interfaces are down.		

Table 36-49 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 1.0.0
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 36-50 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 1.0.0
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 36-51 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 36-52 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 36-53 MplsPathUpdateFailed

Alarm	Attributes	Applicable major release
Name: MplsPathUpdateFailed (1066) Type: pathAlarm Package: mpls.MplsPathUpdateFailed Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mbbRetryExceeded Applicable probable causes: • mbbRetryExceeded • lspPathGoingDown • startingHighPriMbb • restartingMbb • highPriMbbInProg	Release: • 1.0.0
Description: The alarm is raised when an MPLS path update fails because of an MBB problem. The alarm clears when the MBB status changes to Successful.		
Raising condition: (('mbbStatus' NOT EQUAL 'None') AND ('mbbStatus' NOT EQUAL 'Successful'))		
Clearing condition: (('Last Performed State' EQUAL 'Success') OR ('Administrative' EQUAL 'Down') OR (('Operational' EQUAL 'Up') AND ('Last Performed State' EQUAL 'None')))		
Remedial action: Based on the probable cause, change the parameters and update the path again.		

Table 36-54 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		

Table 36-54 MvrSiteDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 36-55 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 1.0.0
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 36-56 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 1.0.0
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		

Table 36-56 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 36-57 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 1.0.0
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 36-58 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 1.0.0
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 36-59 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 1.0.0

Table 36-59 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 36-60 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 36-61 nonDeployedAdjacencyExists

Alarm	Attributes	Applicable major release
Name: nonDeployedAdjacencyExists (11465) Type: communicationsAlarm Package: mpr.nonDeployedAdjacencyExists Raised on class: mpr.BackhaulAdjacency	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonDeployedAdjacencyExists	Release: • 1.0.0
Description: The alarm is raised when a deployed adjacency is deleted on the site.		
Raising condition: (('Deployed to Site' EQUAL 'false') AND ('existedOnSite' EQUAL 'true'))		
Clearing condition: (('Deployed to Site' EQUAL 'true') AND ('existedOnSite' EQUAL 'true'))		
Remedial action: Deploy the changes made to the service.		

Table 36-62 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 1.0.0
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 36-63 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 1.0.0
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 36-64 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 1.0.0
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		

Table 36-64 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 36-65 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 1.0.0
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 36-66 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 1.0.0
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 36-67 PeerConnectionDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerConnectionDown (2) Type: ProtocolAlarm Package: bgp.PeerConnectionDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionDown	Release: • 1.0.0
Description: The alarm is raised when a BGP peer has a Connection State other than Established, and the Administrative State of the BGP peer is Up.		
Raising condition: (('Connection State' NOT EQUAL 'Established') AND ('Administrative State' EQUAL 'Up'))		
Clearing condition: (('Connection State' EQUAL 'Established') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: A mismatch in configuration may have occurred. Check the configuration of both peers to rule out a mismatched configuration.		

Table 36-68 PeerDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerDown (1) Type: ProtocolAlarm Package: bgp.PeerDown Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when a BGP peer has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer entity is down - administratively disable the BGP peer and re-enable it. If toggling the administrative state does not solve the problem check that the physical interface and network connection to the far end peer are up and operational. If the problem persists please contact your Nokia support representative for assistance.		

Table 36-69 PeerGroupDown (bgp)

Alarm	Attributes	Applicable major release
Name: PeerGroupDown (5) Type: ProtocolAlarm Package: bgp.PeerGroupDown Raised on class: bgp.PeerGroup	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when a BGP peer group has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP peer group is down - administratively disable the BGP peer group and re-enable it. If the problem persists please contact your Nokia support representative for assistance.		

Table 36-70 PeerLacIngressEgressFault

Alarm	Attributes	Applicable major release
Name: PeerLacIngressEgressFault (2929) Type: PeerLacAlarm Package: svt.PeerLacIngressEgressFault Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: peerPWStatusBitsChanged	Release: • 1.0.0
Description: The alarm is raised when the Peer Status is Peer LAC Rx Fault and Peer LAC Tx Fault		
Raising condition: (('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault'))		
Clearing condition: NOT ((('Peer State Cause'anyBit'Peer LAC Tx Fault') AND ('Peer State Cause'anyBit'Peer LAC Rx Fault')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 36-71 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 1.0.0
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 36-72 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 36-72 PimDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 36-73 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 36-74 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 1.0.0
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 36-75 PrimaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: PrimaryPathLimitReached (457) Type: resourceAlarm Package: equipment.PrimaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 1.0.0
Description: The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached.		
Raising condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' >=" (1000 * 'Primary Path Limit Override')))"		
Clearing condition: (('Primary Path Limit Override' > '0') AND ('Primary Path In use' < (1000 * 'Primary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management primary path bandwidth limit is reached. This can be remedied by modifying the primary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the primary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 36-76 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 1.0.0
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 36-77 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 1.0.0
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		

Table 36-77 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 36-78 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • 1.0.0
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 36-79 RouteDistinguisherNotConfigured

Alarm	Attributes	Applicable major release
Name: RouteDistinguisherNotConfigured (142) Type: configurationAlarm Package: l3fwd.RouteDistinguisherNotConfigured Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeDistinguisherNotConfig-ured	Release: • 1.0.0
Description: The alarm is raised when no RD is configured for an L3 service site.		
Raising condition: ('routeDistinguisher' EQUAL '\"00 00 00 00 00 00 00 00\"')		
Clearing condition: ('routeDistinguisher' NOT EQUAL '\"00 00 00 00 00 00 00 00\"')		
Remedial action: A configuration error has occurred which must be corrected. The RD must be configured on the L3 Service Site in question.		

Table 36-80 RsvpDown

Alarm	Attributes	Applicable major release
Name: RsvpDown (74) Type: ProtocolAlarm Package: rsvp.RsvpDown Raised on class: rsvp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 1.0.0

Table 36-80 RsvpDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an RSVP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RSVP Site is down while it is administratively up. Please check MPLS is enabled and administratively up.		

Table 36-81 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 1.0.0
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 36-82 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 36-83 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 1.0.0
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 36-84 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 1.0.0
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 36-85 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 1.0.0
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		

Table 36-85 SdpEgressIfsNetDomainInConsistent (continued)

Alarm	Attributes	Applicable major release
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 36-86 SecondaryPathLimitReached

Alarm	Attributes	Applicable major release
Name: SecondaryPathLimitReached (458) Type: resourceAlarm Package: equipment.SecondaryPathLimitReached Raised on class: equipment.DaughterCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 1.0.0
Description: The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached.		
Raising condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' >=" (1000 * 'Secondary Path Limit Override')))"		
Clearing condition: (('Secondary Path Limit Override' > '0') AND ('Secondary Path In use' < (1000 * 'Secondary Path Limit Override')))		
Remedial action: Informational - The alarm is raised when the Ingress Multicast Path Management secondary path bandwidth limit is reached. This can be remedied by modifying the secondary path limit located at T1 Paths tab of the multicast bandwidth policy which assigned to the card, or increase the secondary path limit override located at the Daughter Card tab under Daughter Card Slot form.		

Table 36-87 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 1.0.0
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 36-88 SessionDown

Alarm	Attributes	Applicable major release
Name: SessionDown (73) Type: ProtocolAlarm Package: rsvp.SessionDown Raised on class: rsvp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 1.0.0
Description: The alarm is raised when an RSVP session is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Please check the RSVP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 36-89 SingleSFMOverloadDetected

Alarm	Attributes	Applicable major release
Name: SingleSFMOverloadDetected (843) Type: ProtocolAlarm Package: l3fwd.SingleSFMOverloadDetected Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signleSfmOverloadDetected	Release: • 1.0.0
Description: The alarm is raised when a device reports a single-SFM overload. The alarm clears when the VR exits the Overload state.		
Raising condition: ('Overload State' EQUAL 'Overload')		
Clearing condition: ('Overload State' EQUAL 'Normal')		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 36-90 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 36-91 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 1.0.0
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 36-92 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 1.0.0
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 36-93 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 1.0.0
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		

Table 36-93 TemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 36-94 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 36-95 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 1.0.0
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 36-95 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 36-96 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 1.0.0
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 36-97 TunnelAdministrativelyDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: mpls.TunnelAdministrativelyDown Raised on class: mpls.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 1.0.0

Table 36-97 TunnelAdministrativelyDown (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects that an MPLS path is administratively down.		
Raising condition: ('Administrative' NOT EQUAL 'Up')		
Clearing condition: ('Administrative' EQUAL 'Up')		
Remedial action: Turn up the corresponding MPLS path.		

Table 36-98 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 36-99 TunnelDown (mpls)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: mpls.TunnelDown Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 1.0.0
Description: The alarm is raised when an MPLS path has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: Check the network resources along the path.		

Table 36-100 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 1.0.0
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 36-101 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 1.0.0
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 36-102 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 1.0.0
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 36-103 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 1.0.0
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 36-104 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 1.0.0
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 36-105 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 1.0.0
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 36-106 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 1.0.0
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 36-107 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 1.0.0
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 36-108 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 1.0.0
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

Table 36-109 XplError

Alarm	Attributes	Applicable major release
Name: XplError (573) Type: hardwareAnomaly Package: equipment.XplError Raised on class: equipment.DaughterCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: xplError	Release: • 1.0.0
Description: The alarm is raised when an MDA reports persistent XPL Errors.		
Raising condition: ('Number Of Notifications' NOT EQUAL '0')		
Clearing condition: ('Number Of Notifications' EQUAL '0')		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

37 HIP

37.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 37-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • N/A
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 37-2 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • N/A
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 37-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • N/A
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 37-4 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 37-5 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • N/A
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		

Table 37-5 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 37-6 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 37-7 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 37-8 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • N/A
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 37-9 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 37-10 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • N/A

Table 37-10 CmuManagementFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 37-11 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 37-12 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 37-13 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 37-14 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • N/A
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 37-15 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • N/A
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		

Table 37-15 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 37-16 EMSNetworkElementSystemAlarmOverLoad

Alarm	Attributes	Applicable major release
Name: EMSNetworkElementSystemAlarmOverLoad (4620) Type: processingErrorAlarm Package: hip.EMSNetworkElementSystemAlarmOverLoad Raised on class: hip.EMSNetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemResourcesOverload	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects an overload of EMS alarms in the alarm list.		
Raising condition: ('alarmOverLoaded' EQUAL 'true')		
Clearing condition: ('alarmOverLoaded' EQUAL 'false')		
Remedial action: Informational - no corrective action required.		

Table 37-17 EMSNetworkElementSystemUnreachable

Alarm	Attributes	Applicable major release
Name: EMSNetworkElementSystemUnreachable (4621) Type: communicationsAlarm Package: hip.EMSNetworkElementSystemUnreachable Raised on class: hip.EMSNetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError Applicable probable causes: • connectionEstablishmentError • transmissionError • fireDetected • lossOfRedundancy • protectionMechanismFailure • protectingResourceFailure • excessiveResponseTime • excessiveRetransmissionRate	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a HIP communication link failure to the EM System while the EM System is administratively up. The alarm clears when the HIP link returns to service or the EM System is no longer administratively up.		
Raising condition: ('alarmNetworkConnection' EQUAL 'true')		
Clearing condition: ('alarmNetworkConnection' EQUAL 'false')		

Table 37-17 EMSNetworkElementSystemUnreachable (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check network connectivity between the SAM main server and EM System server. Check that the EM System is running and connectivity to SAM is operational.		

Table 37-18 EMSystemAlarmOverLoad

Alarm	Attributes	Applicable major release
Name: EMSystemAlarmOverLoad (3741) Type: processingErrorAlarm Package: hip.EMSystemAlarmOverLoad Raised on class: hip.EMSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemResourcesOverload	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects an overload of EMS alarms in the alarm list.		
Raising condition: ('alarmOverLoaded' EQUAL 'true')		
Clearing condition: ('alarmOverLoaded' EQUAL 'false')		
Remedial action: Informational - no corrective action required.		

Table 37-19 EMSystemTimeOut

Alarm	Attributes	Applicable major release
Name: EMSystemTimeOut (8151) Type: communicationsAlarm Package: hip.EMSystemTimeOut Raised on class: hip.EMSystem	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: excessiveResponseTime	Release: • N/A
Description: The alarm is raised when the time out is raised (the SAM to EMS request take too long time)		
Remedial action: NA		

Table 37-20 EMSystemUnreachable

Alarm	Attributes	Applicable major release
Name: EMSystemUnreachable (2947) Type: communicationsAlarm Package: hip.EMSystemUnreachable Raised on class: hip.EMSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError Applicable probable causes: • connectionEstablishmentError • transmissionError • fireDetected • lossOfRedundancy • protectionMechanismFailure • protectingResourceFailure • excessiveResponseTime • excessiveRetransmissionRate	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a HIP communication link failure to the EM System while the EM System is administratively up. The alarm clears when the HIP link returns to service or the EM System is no longer administratively up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Network Connection Status' NOT EQUAL 'Up'))		
Clearing condition: (('Administrative State' NOT EQUAL 'Up') OR ('Network Connection Status' EQUAL 'Up'))		
Remedial action: Check network connectivity between the SAM main server and EM System server. Check that the EM System is running and connectivity to SAM is operational.		

Table 37-21 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 37-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 37-23 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • N/A
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 37-24 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • N/A
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		

Table 37-24 EquipmentInTest (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 37-25 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 37-26 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 37-27 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • N/A
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		

Table 37-27 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 37-28 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • N/A
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 37-29 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 37-30 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • N/A
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 37-31 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 37-32 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • N/A
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 37-33 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • N/A
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 37-34 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • N/A
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 37-35 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • N/A
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 37-35 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 37-36 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 37-37 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • N/A
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 37-38 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • N/A
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 37-39 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 37-40 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • N/A
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 37-41 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • N/A
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 37-42 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • N/A
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 37-43 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • N/A
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		

Table 37-43 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 37-44 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 37-45 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • N/A
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 37-46 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • N/A
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 37-47 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • N/A
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 37-48 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • N/A
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 37-49 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • N/A
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 37-50 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 37-51 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 37-52 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • N/A
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 37-53 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • N/A
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 37-54 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		

Table 37-54 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 37-55 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • N/A
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 37-56 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw.TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • N/A
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 37-57 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • N/A
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 37-58 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • N/A

Table 37-58 UnmanageFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 37-59 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • N/A
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 37-60 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • N/A
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 37-61 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • N/A
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 37-62 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • N/A
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 37-63 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • N/A
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 37-64 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • N/A
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

38 FlexiPacket Hub 800

38.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 38-1 AccountLogFilledFirstThreshold

Alarm	Attributes	Applicable major release
Name: AccountLogFilledFirstThreshold (11470) Type: processingErrorAlarm Package: netw.AccountLogFilledFirstThreshold Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when the first threshold on account log is crossed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-2 AccountLogFilledSecondThreshold

Alarm	Attributes	Applicable major release
Name: AccountLogFilledSecondThreshold (11471) Type: processingErrorAlarm Package: netw.AccountLogFilledSecondThreshold Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when the second threshold on account log is crossed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-3 AutonegotiationMismatch

Alarm	Attributes	Applicable major release
Name: AutonegotiationMismatch (11282) Type: communicationsAlarm Package: equipment.AutonegotiationMismatch Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when there is Autonegotiation mismatch on the GbE interface.		

Table 38-3 AutonegotiationMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-4 CardDisconnected

Alarm	Attributes	Applicable major release
Name: CardDisconnected (11283) Type: equipmentAlarm Package: equipment.CardDisconnected Raised on class: equipment.CardSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when the Card status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-5 CardMismatchIndication

Alarm	Attributes	Applicable major release
Name: CardMismatchIndication (11284) Type: equipmentAlarm Package: equipment.CardMismatchIndication Raised on class: equipment.CardSlot	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when the Card status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-6 CCMContinuityCheckLoss

Alarm	Attributes	Applicable major release
Name: CCMContinuityCheckLoss (11245) Type: equipmentAlarm Package: dw.CCMContinuityCheckLoss Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when the IDU does not receive nsncetCfmMepCClossThreshold consecutive CCMs in the relevant MEP. 'nsncetCfmMepCClossThreshold' is the Number of missed CCMs that cause some CCM defect.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-7 DebugModeOn

Alarm	Attributes	Applicable major release
Name: DebugModeOn (11475) Type: processingErrorAlarm Package: netw.DebugModeOn Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when the Node is set to Debug Mode.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-8 E1AISIn

Alarm	Attributes	Applicable major release
Name: E1AISIn (11285) Type: communicationsAlarm Package: equipment.E1AISIn Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-9 E1AISOut

Alarm	Attributes	Applicable major release
Name: E1AISOut (11286) Type: communicationsAlarm Package: equipment.E1AISOut Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-10 E1FarEndFailure

Alarm	Attributes	Applicable major release
Name: E1FarEndFailure (11287) Type: communicationsAlarm Package: equipment.E1FarEndFailure Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-11 E1LoF

Alarm	Attributes	Applicable major release
Name: E1LoF (11288) Type: communicationsAlarm Package: equipment.E1LoF Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoF	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-12 E1LoS

Alarm	Attributes	Applicable major release
Name: E1LoS (11289) Type: communicationsAlarm Package: equipment.E1LoS Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoS	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-13 E1MaintenanceLoopback

Alarm	Attributes	Applicable major release
Name: E1MaintenanceLoopback (11290) Type: equipmentAlarm Package: equipment.E1MaintenanceLoopback Raised on class: equipment.PhysicalPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Maintenance	Release: • N/A
Description: This alarm is sent when the value of Line Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-14 LocalSignalFailure

Alarm	Attributes	Applicable major release
Name: LocalSignalFailure (11249) Type: communicationsAlarm Package: dw.LocalSignalFailure Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is generated on the following events: - Local SF is received for the ring. - Local Clear SF is received for the ring.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-15 ManualOperationOn

Alarm	Attributes	Applicable major release
Name: ManualOperationOn (11481) Type: processingErrorAlarm Package: netw.ManualOperationOn Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is related to Test/Manual Operation. It is raised when at least one test configuration is active.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-16 MEP1731AIS

Alarm	Attributes	Applicable major release
Name: MEP1731AIS (11250) Type: equipmentAlarm Package: dw.MEP1731AIS Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm indicates MEP is in AIS Condition. AIS condition occurs when the interface receives an AIS frame.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-17 MPTermination

Alarm	Attributes	Applicable major release
Name: MPTermination (11251) Type: communicationsAlarm Package: dw.MPTermination Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during the notification of LCP link termination.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-18 NEOverheating

Alarm	Attributes	Applicable major release
Name: NEOverheating (11485) Type: equipmentAlarm Package: netw.NEOverheating Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A

Table 38-18 NEOverheating (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the board temperature is higher than the threshold. This is the internally measured temperature, which has a delta with respect to environmental temperature of about 20C more. If the internal temperature rises up to 75C, system will report the Equipment OverHeating alarm; if the internal temperature falls below 72C, system will clear the Equipment OverHeating alarm. Resolution 1 degree; check every 15s.'		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-19 NoPowerSupplyToODU

Alarm	Attributes	Applicable major release
Name: NoPowerSupplyToODU (11294) Type: equipmentAlarm Package: equipment.NoPowerSupplyToODU Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when PW Supply to ODU has failed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-20 OAMDiscoveryFail

Alarm	Attributes	Applicable major release
Name: OAMDiscoveryFail (11808) Type: communicationsAlarm Package: equipment.OAMDiscoveryFail Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when the Local NE cannot detect the presence of an OAM sublayer at the remote NE. In passive mode, NE doesn't receive OAMPDU after three intervals after admin enabling. In active mode, NE doesn't receive OAMPDU after three intervals after admin enabling OR Negotiation failed after receiving Information OAMPDU. This alarm is cleared when negotiation process is successful.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-21 OAMMAConfigurationError

Alarm	Attributes	Applicable major release
Name: OAMMAConfigurationError (11252) Type: qualityOfServiceAlarm Package: dw.OAMMAConfigurationError Raised on class: dw.DwAlarmedObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: QoSError	Release: • N/A
Description: This alarm is raised when the content of a received CCM message is not coherent with the configuration.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-22 OpticalSFPLoS

Alarm	Attributes	Applicable major release
Name: OpticalSFPLoS (11295) Type: communicationsAlarm Package: equipment.OpticalSFPLoS Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoS	Release: • N/A
Description: This alarm is raised when SFP LOS is active. This is applicable only for Optical SFP ports.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-23 OpticalSFPTXFault

Alarm	Attributes	Applicable major release
Name: OpticalSFPTXFault (11296) Type: equipmentAlarm Package: equipment.OpticalSFPTXFault Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when SFP Tx Fault is active. This is applicable only for Optical SFP ports.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-24 OvercurrentOrUndercurrentFPRPowerSupply

Alarm	Attributes	Applicable major release
Name: OvercurrentOrUndercurrentFPRPowerSupply (11297) Type: equipmentAlarm Package: equipment. OvercurrentOrUndercurrentFPRPowerSupply Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when Overcurrent/Undercurrent condition is detected at the ODU Ethernet Interface. Possible causes: (a) Short/open circuit in ODU cable (b) Wrong cable manifacturing; (c) ODU failure.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-25 PortDown

Alarm	Attributes	Applicable major release
Name: PortDown (11299) Type: communicationsAlarm Package: equipment.PortDown Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • N/A

Table 38-25 PortDown (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the Operational State of Port goes down when the Admin State is up.		
Remedial action: Please refer to Troubleshooting Guide for remedial action.		

Table 38-26 PortFail

Alarm	Attributes	Applicable major release
Name: PortFail (11300) Type: equipmentAlarm Package: equipment.PortFail Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised to indicate the Media Availability State on the GbE interface. The states are as per definitions in IANA-MAU MIB.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-27 PortSpeedLower

Alarm	Attributes	Applicable major release
Name: PortSpeedLower (11301) Type: qualityOfServiceAlarm Package: equipment.PortSpeedLower Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: QoSError	Release: • N/A
Description: This alarm is raised when the Interface Speed is less than the absolute shaped bandwidth of the Interface.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-28 PortSpeedLowerThanCIR

Alarm	Attributes	Applicable major release
Name: PortSpeedLowerThanCIR (11302) Type: qualityOfServiceAlarm Package: equipment.PortSpeedLowerThanCIR Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: QoSError	Release: • N/A
Description: This alarm is raised when the Interface Speed is less than sum of CIR of allocated services on the Interface.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-29 PowerSupplyToODUFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyToODUFailure (11303) Type: equipmentAlarm Package: equipment.PowerSupplyToODUFailure Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when PW Supply to ODU has failed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-30 PowerSupplyToODUShortCircuit

Alarm	Attributes	Applicable major release
Name: PowerSupplyToODUShortCircuit (11304) Type: equipmentAlarm Package: equipment.PowerSupplyToODUShortCircuit Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when PW Supply to ODU has failed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-31 PWFail

Alarm	Attributes	Applicable major release
Name: PWFail (11257) Type: equipmentAlarm Package: dw.PWFail Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when the OperStatus object for one or more PW objects are about to enter the down or lowerLayerDown state from any other state, except for transition from the notPresent state.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-32 PWFunctionAlarm

Alarm	Attributes	Applicable major release
Name: PWFunctionAlarm (11489) Type: equipmentAlarm Package: netw.PWFunctionAlarm Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised as soon as OperStatus on any one PW is not up while its relevant AdminStatus is enabled. It is cleared when OperStatus on all PW objectes are up for which the corresponding AdmimState is enabled.		

Table 38-32 PWFunctionAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-33 PWRemotePacketLoss

Alarm	Attributes	Applicable major release
Name: PWRemotePacketLoss (11258) Type: communicationsAlarm Package: dw.PWRemotePacketLoss Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when there is Remote Packet Loss Indication on the PW object.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-34 RadioLinkStatusDown

Alarm	Attributes	Applicable major release
Name: RadioLinkStatusDown (11262) Type: communicationsAlarm Package: dw.RadioLinkStatusDown Raised on class: dw.DwAlarmedObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CommunicationError	Release: • N/A
Description: This alarm is raised when the Radio Link status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-35 RemoteFaultIndication

Alarm	Attributes	Applicable major release
Name: RemoteFaultIndication (11306) Type: communicationsAlarm Package: equipment.RemoteFaultIndication Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when there is remote fault. It means that the partner connected to the port is signalling a fault.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-36 RemoteSignalFailure

Alarm	Attributes	Applicable major release
Name: RemoteSignalFailure (11263) Type: communicationsAlarm Package: dw.RemoteSignalFailure Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is generated on the following events: - Remote failure is detected on this ring. - Remote failure is cleared on this ring.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-37 RingFailure

Alarm	Attributes	Applicable major release
Name: RingFailure (11491) Type: communicationsAlarm Package: netw.RingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is generated when there is any failure on a ring.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-38 ScheduledActionFailure

Alarm	Attributes	Applicable major release
Name: ScheduledActionFailure (11272) Type: processingErrorAlarm Package: dw.ScheduledActionFailure Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is generated whenever a scheduled operation has failed.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-39 SelfTestFailure

Alarm	Attributes	Applicable major release
Name: SelfTestFailure (11494) Type: processingErrorAlarm Package: netw.SelfTestFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when the self test procedure fails.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-40 ServiceDown

Alarm	Attributes	Applicable major release
Name: ServiceDown (11273) Type: qualityOfServiceAlarm Package: dw.ServiceDown Raised on class: dw.DwAlarmedObject	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ServiceError	Release: • N/A
Description: This alarm is raised when the Operation State of Service is Down. For E-LINE service, alarm is raised under following conditions - (a) If the service SubType is 'p2p' - no connectivity with the other end-point. (b) If the service SubType is 'tls' - no connectivity with a VPLS VSI. For E-LAN service, the alarm is raised when service has no end-to-end connectivity.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-41 ServicePartial

Alarm	Attributes	Applicable major release
Name: ServicePartial (11274) Type: qualityOfServiceAlarm Package: dw.ServicePartial Raised on class: dw.DwAlarmedObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: QoSError	Release: • N/A
Description: This alarm is raised when the Service State changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-42 SFPAbsent

Alarm	Attributes	Applicable major release
Name: SFPAbsent (11307) Type: equipmentAlarm Package: equipment.SFPAbsent Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when SFP module is missing.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-43 SFPMismatch

Alarm	Attributes	Applicable major release
Name: SFPMismatch (11308) Type: equipmentAlarm Package: equipment.SFPMismatch Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when there is SFP mismatch.		

Table 38-43 SFPMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-44 SFPRxPowerAbnormal

Alarm	Attributes	Applicable major release
Name: SFPRxPowerAbnormal (11309) Type: equipmentAlarm Package: equipment.SFPRxPowerAbnormal Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when Calibrated Rx Power value is bigger than the higher threshold or lower than lower threshold. This alarm is evaluated if and only if the SFPMissing and SFPMismatch alarms are not raised.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-45 SFPTxPowerAbnormal

Alarm	Attributes	Applicable major release
Name: SFPTxPowerAbnormal (11310) Type: equipmentAlarm Package: equipment.SFPTxPowerAbnormal Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyError	Release: • N/A
Description: This alarm is raised when Calibrated Tx Power value is bigger than the higher threshold or lower than lower threshold configured. This alarm is evaluated if and only if the SFPMissing and SFPMismatch alarms are not raised.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-46 SoftwareSwitchNotAllowed

Alarm	Attributes	Applicable major release
Name: SoftwareSwitchNotAllowed (11495) Type: processingErrorAlarm Package: netw.SoftwareSwitchNotAllowed Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: This alarm is raised when Switching action is initiated when not allowed. When any component Standby FW version is not compatible with the HW version, the switch command can not be executed. A new software must be downloaded.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-47 StationAlarmOn

Alarm	Attributes	Applicable major release
Name: StationAlarmOn (11496) Type: processingErrorAlarm Package: netw.StationAlarmOn Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProcessingError	Release: • N/A
Description: Station Alarm.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-48 STM1AuAIS

Alarm	Attributes	Applicable major release
Name: STM1AuAIS (11312) Type: communicationsAlarm Package: equipment.STM1AuAIS Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-49 STM1AULossOfPointer

Alarm	Attributes	Applicable major release
Name: STM1AULossOfPointer (11311) Type: communicationsAlarm Package: equipment.STM1AULossOfPointer Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-50 STM1HighPathSignalLabelMismatch

Alarm	Attributes	Applicable major release
Name: STM1HighPathSignalLabelMismatch (11317) Type: communicationsAlarm Package: equipment. STM1HighPathSignalLabelMismatch Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-51 STM1HPDegrade

Alarm	Attributes	Applicable major release
Name: STM1HPDegrade (11313) Type: communicationsAlarm Package: equipment.STM1HPDegrade Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when the Path is Degraded.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-52 STM1HPExcessiveError

Alarm	Attributes	Applicable major release
Name: STM1HPExcessiveError (11314) Type: communicationsAlarm Package: equipment.STM1HPExcessiveError Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during Path Excessive Error.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-53 STM1HPRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: STM1HPRemoteDefectIndication (11315) Type: communicationsAlarm Package: equipment.STM1HPRemoteDefectIndication Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-54 STM1HPUnequipped

Alarm	Attributes	Applicable major release
Name: STM1HPUnequipped (11316) Type: equipmentAlarm Package: equipment.STM1HPUnequipped Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-55 STM1J0TraceIdentifierMismatch

Alarm	Attributes	Applicable major release
Name: STM1J0TraceIdentifierMismatch (11318) Type: communicationsAlarm Package: equipment.STM1J0TraceIdentifierMismatch Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during J0 TIM event.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-56 STM1J1TraceIdentifierMismatch

Alarm	Attributes	Applicable major release
Name: STM1J1TraceIdentifierMismatch (11319) Type: communicationsAlarm Package: equipment.STM1J1TraceIdentifierMismatch Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during J1 TIM event.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-57 STM1LoF

Alarm	Attributes	Applicable major release
Name: STM1LoF (11320) Type: communicationsAlarm Package: equipment.STM1LoF Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoF	Release: • N/A
Description: This alarm is raised when the RS Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-58 STM1LoS

Alarm	Attributes	Applicable major release
Name: STM1LoS (11321) Type: communicationsAlarm Package: equipment.STM1LoS Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoS	Release: • N/A
Description: This alarm is raised when the RS Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-59 STM1LpDegrade

Alarm	Attributes	Applicable major release
Name: STM1LpDegrade (11265) Type: communicationsAlarm Package: dw.STM1LpDegrade Raised on class: dw.DwIduVC12Specifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when VC12 is degraded.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-60 STM1LPJ2TraceIdentifierMismatch

Alarm	Attributes	Applicable major release
Name: STM1LPJ2TraceIdentifierMismatch (11264) Type: communicationsAlarm Package: dw.STM1LPJ2TraceIdentifierMismatch Raised on class: dw.DwIduVC12Specifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during J2 TIM event.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-61 STM1LpRemoteDefectIndication

Alarm	Attributes	Applicable major release
Name: STM1LpRemoteDefectIndication (11266) Type: communicationsAlarm Package: dw.STM1LpRemoteDefectIndication Raised on class: dw.DwIduVC12Specifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-62 STM1LpRemoteFailureIndication

Alarm	Attributes	Applicable major release
Name: STM1LpRemoteFailureIndication (11267) Type: communicationsAlarm Package: dw.STM1LpRemoteFailureIndication Raised on class: dw.DwIduVC12Specifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-63 STM1LpSignalLabelMismatch

Alarm	Attributes	Applicable major release
Name: STM1LpSignalLabelMismatch (11268) Type: communicationsAlarm Package: dw.STM1LpSignalLabelMismatch Raised on class: dw.DwIduVC12Specifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-64 STM1LpTuAIS

Alarm	Attributes	Applicable major release
Name: STM1LpTuAIS (11269) Type: communicationsAlarm Package: dw.STM1LpTuAIS Raised on class: dw.DwIduVC12Specifics	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-65 STM1LpTuLossOfMultiframe

Alarm	Attributes	Applicable major release
Name: STM1LpTuLossOfMultiframe (11322) Type: communicationsAlarm Package: equipment.STM1LpTuLossOfMultiframe Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during STM1#n LP#m TU loss of multiframe.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-66 STM1LpTuLossOfPointer

Alarm	Attributes	Applicable major release
Name: STM1LpTuLossOfPointer (11270) Type: communicationsAlarm Package: dw.STM1LpTuLossOfPointer Raised on class: dw.DwIduVC12Specifics	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-67 STM1LpUnequipped

Alarm	Attributes	Applicable major release
Name: STM1LpUnequipped (11271) Type: communicationsAlarm Package: dw.STM1LpUnequipped Raised on class: dw.DwIduVC12Specifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised when VC4 Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-68 STM1MSAIS

Alarm	Attributes	Applicable major release
Name: STM1MSAIS (11323) Type: communicationsAlarm Package: equipment.STM1MSAIS Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AIS	Release: • N/A
Description: This alarm is raised when MS Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-69 STM1MSDegrade

Alarm	Attributes	Applicable major release
Name: STM1MSDegrade (11324) Type: communicationsAlarm Package: equipment.STM1MSDegrade Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during MS Degrade.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-70 STM1MSExcessiveError

Alarm	Attributes	Applicable major release
Name: STM1MSExcessiveError (11325) Type: communicationsAlarm Package: equipment.STM1MSExcessiveError Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during Multiplex Section Excessive Error event.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-71 STM1MSFarEndFailure

Alarm	Attributes	Applicable major release
Name: STM1MSFarEndFailure (11326) Type: communicationsAlarm Package: equipment.STM1MSFarEndFailure Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FarEndFailure	Release: • N/A
Description: This alarm is raised when MS Status changes.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-72 STM1RSDegrade

Alarm	Attributes	Applicable major release
Name: STM1RSDegrade (11327) Type: communicationsAlarm Package: equipment.STM1RSDegrade Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignallingError	Release: • N/A
Description: This alarm is raised during RS Degrade.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-73 SwHwMismatch

Alarm	Attributes	Applicable major release
Name: SwHwMismatch (11497) Type: equipmentAlarm Package: netw.SwHwMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised to indicate Software/Firmware and Hardware mismatch. This occurs when the loaded SW and FW is not compatible with HW.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-74 SynchAllSourcesDown

Alarm	Attributes	Applicable major release
Name: SynchAllSourcesDown (11498) Type: communicationsAlarm Package: netw.SynchAllSourcesDown Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A

Table 38-74 SynchAllSourcesDown (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when a physical layer problem in all the configured synchronization interfaces is detected. Possible causes for IDU: (a) LinkState="DOWN has been detected in the Ethernet interface selected as synchronization interface. (b) LOS has been detected in the E1 interface selected as synchronization interface. As a consequent action the equipment will go to holdover state. The alarm is masked when the system is in Internal Synchronization Mode. Possible causes for ODU: The MultiRadio ODU has detected a physical layer problem in all the configured synchronization interfaces. As a consequent action the equipment will go to holdover state. Action: Check the synchronization sources."		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-75 SynchConfigurationError

Alarm	Attributes	Applicable major release
Name: SynchConfigurationError (11275) Type: communicationsAlarm Package: dw.SynchConfigurationError Raised on class: dw.ClockSource	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: This alarm is raised when the Node is receiving SSM carrying a DNU code from at least one synchronization interface. Possible cause: misconfiguration of the peer equipment. The alarm is masked when the SSM are disabled for that interface.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-76 SynchMissingSSM

Alarm	Attributes	Applicable major release
Name: SynchMissingSSM (11276) Type: communicationsAlarm Package: dw.SynchMissingSSM Raised on class: dw.ClockSource	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: The equipment activates this alarm when it does not receive SSM messages from the selected synchronization interface. When multiple interfaces are configured as synchronization sources this alarm is activated if it does not receive SSM messages from at least one of the configured synchronization interfaces. Possible causes: misconfiguration of the peer equipment. The alarm is masked when the SSM are disabled for that interface.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-77 SynchOneSourceDown (dw)

Alarm	Attributes	Applicable major release
Name: SynchOneSourceDown (11277) Type: communicationsAlarm Package: dw.SynchOneSourceDown Raised on class: dw.ClockSource	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A

Table 38-77 SynchOneSourceDown (dw) (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when when multiple synchronization interfaces are configured AND a physical layer problem in at least one of the synchronization interfaces is detected. Possible causes: (a) LinkState="DOWN has been detected in an Ethernet interface selected as synchronization interface (b) LOS has been detected in the E1 interface selected as synchronization interface. As a consequent action the equipment will select the alternative synchronization source. The alarm is masked when the system is in Internal Synchronization Mode. The alarm is masked when the flexiPacketIDUSeInterfAllDown is active."		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-78 SynchQualityLevelDegraded

Alarm	Attributes	Applicable major release
Name: SynchQualityLevelDegraded (11278) Type: qualityOfServiceAlarm Package: dw.SynchQualityLevelDegraded Raised on class: dw.ClockSource	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: The equipment activates this alarm when it receives SSM messages from the selected synchronization interface carrying a quality code lower than the expected one. Possible causes: (a) failure of the upstream synchronization network (b) equipment misconfiguration. The alarm is masked when the SSM are disabled for that interface.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-79 SynchUnlockedPLL

Alarm	Attributes	Applicable major release
Name: SynchUnlockedPLL (11499) Type: communicationsAlarm Package: netw.SynchUnlockedPLL Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: The equipment activates this alarm when it has been configured in External Reference mode, but the PLL is unlocked. Possible causes: (a) the local oscillator is out-of-range (b) the uplink device is out-of-range. The alarm is masked when the system is in Internal Synchronization Mode.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-80 SystemFailure

Alarm	Attributes	Applicable major release
Name: SystemFailure (11500) Type: equipmentAlarm Package: netw.SystemFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EquipmentError	Release: • N/A
Description: This alarm is raised to indicate Equipment Failure. The FPH 800 IDU is Out of Service and needs to be replaced.		

Table 38-80 SystemFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-81 TimeServerMissing

Alarm	Attributes	Applicable major release
Name: TimeServerMissing (11503) Type: communicationsAlarm Package: netw.TimeServerMissing Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncError	Release: • N/A
Description: This alarm is raised when the Time Server is missing. Cleared when time server answers. Action: Check the cable.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-82 TrapOutOfSequence

Alarm	Attributes	Applicable major release
Name: TrapOutOfSequence (11504) Type: equipmentAlarm Package: netw.TrapOutOfSequence Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingTrap	Release: • N/A
Description: This alarm is raised when SAM receives a trap that is out of sequence. This indicates some trap(s) sent from node did not reach SAM. When SAM receives an alarm that is out of sequence, SAM automaticlally synchronizes the Active Alarms on the Node and state information (Admin and Oper states) on all Ports. However, if any traps related to equipment configuration and service do not reach SAM, Full Node Sync needs to be manually triggered in order to synchronize Node with SAM.		
Remedial action: Please trigger Full Node Synchronization on the Node.		

Table 38-83 USBKeyForWrongNEType

Alarm	Attributes	Applicable major release
Name: USBKeyForWrongNEType (11506) Type: equipmentAlarm Package: netw.USBKeyForWrongNEType Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: USBKeyError	Release: • N/A
Description: This alarm is raised when the Memory key is invalid. Memory key is considered not valid due to a different Equipment Type stored information. The equipment enters the Idle state if invalid valid key is detected at start-up, whereas it stays in the previous state (Idle or run/no set) if the not valid key is detected during run time (a wrong key has been plugged into the appliance).		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-84 USBKeyNotPresent

Alarm	Attributes	Applicable major release
Name: USBKeyNotPresent (11507) Type: equipmentAlarm Package: netw.USBKeyNotPresent Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: USBKeyError	Release: • N/A
Description: This alarm is raised when the availability of USB Key physical device is no more detected during run-time polling or at startup. The equipment enters the Idle state if the absence is detected at start-up, whereas it enters the Run/no set state if the absence is detected during run time.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-85 USBKeyOverload

Alarm	Attributes	Applicable major release
Name: USBKeyOverload (11508) Type: equipmentAlarm Package: netw.USBKeyOverload Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: USBKeyError	Release: • N/A
Description: This alarm is raised when the unused space in USB key less than 30M. Cleared when the unused space in USB key is more than 50M. When this alarm occurs, it is suggested to remove the unused files.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

Table 38-86 USBKeyWithMismatchContent

Alarm	Attributes	Applicable major release
Name: USBKeyWithMismatchContent (11509) Type: equipmentAlarm Package: netw.USBKeyWithMismatchContent Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: USBKeyError	Release: • N/A
Description: This alarm is raised when the System type stored in the Memory Key is not supported by the NE embedded SW. This can be detected at start-up only, thus controller enters the Idle state.		
Remedial action: Please refer to Harmony Hub800 Troubleshooting Guide for remedial action.		

39 Unspecified NE

39.1 Alarms

Alarms

Note: This chapter lists alarms that have no NE type specified. The alarms listed in this chapter may apply to one or more NE types, however, this information is not specified in the 5620 SAM alarm schema. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort.

Table 39-1 AARadiusAcctPlcyFailure

Alarm	Attributes	Applicable major release
Name: AARadiusAcctPlcyFailure (3948) Type: AARadiusAcctPlcyFailureAlarm Package: aapolicy.AARadiusAcctPlcyFailure Raised on class: aapolicy.AARadiusAccountingPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: aARadiusAcctPlcyFailure	Release: • N/A
Description: The alarm is raised when a RADIUS accounting request was not successfully sent to any of the RADIUS servers specified in the AA RADIUS accounting policy. The effect is accounting data for current subscribers will not be exported externally. Based on the noted reason, if necessary take action to ensure that the next RADIUS accounting will be successfully sent.		
Remedial action: The AA RADIUS Accounting Server(s) which are configured in the AA RADIUS Accounting Policy are unreachable. This may occur in a number of different scenarios. The server(s) may have become unresponsive - please refer to the AA RADIUS Accounting Server documentation for assistance. The network connectivity to the server(s) may have been lost - please investigate why the underlying transport network is unreliable.		

Table 39-2 AARadiusAcctServerStateChanged

Alarm	Attributes	Applicable major release
Name: AARadiusAcctServerStateChanged (3949) Type: AARadiusAcctServerStateChangedAlarm Package: aapolicy.AARadiusAcctServerStateChanged Raised on class: aapolicy.AARadiusAccountingServer	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aARadiusAcctServerStat-eChanged	Release: • N/A
Description: The notification alarm is raised when the operational status of an AA RADIUS Accounting Policy Server has transitioned from 'In Service' to 'Out of Service' or 'Unknown' and cleared when operational status transitioned to 'In Service'.		
Raising condition: (('Operational State' EQUAL 'Out Of Service') AND ('isLocal' EQUAL 'true'))		
Clearing condition: ('Operational State' EQUAL 'In Service')		
Remedial action: Informational - This is a notification alarm to indicate that AA RADIUS Accounting Server which is configured in the AA RADIUS Accounting Policy is changing operational state.		

Table 39-3 AarpStateChanged

Alarm	Attributes	Applicable major release
Name: AarpStateChanged (3705) Type: AarpStateChanged Package: aapolicy.AarpStateChanged Raised on class: aapolicy.Aarp	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AarpStateChanged	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects that an AARP state is changed.		
Remedial action: The application assurance redundancy protocol state is changed between standalone, remote, master or backup.		

Table 39-4 AaStatTcaCfgThrshCross

Alarm	Attributes	Applicable major release
Name: AaStatTcaCfgThrshCross (9634) Type: processingErrorAlarm Package: aapolicy.AaStatTcaCfgThrshCross Raised on class: aapolicy.AaStatTcaCfg	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aaStatTcaCfgThrshCross	Release: • N/A
Description: The alarm is generated when the utilization matching a AaStatTcaCfg in the past minute is greater than or equal to the value of tcaHighWatermark and the notification is not currently raised for the same entry.		
Remedial action: The utilization of the AA Statistics TCA Config(s) which are configured in the AA Statistics TCA Config Policy are equal or higher than the configured high watermark. Make an adjustment to the watermark.		

Table 39-5 AaStatTcaFilterThrshCross

Alarm	Attributes	Applicable major release
Name: AaStatTcaFilterThrshCross (9635) Type: processingErrorAlarm Package: aapolicy.AaStatTcaFilterThrshCross Raised on class: aapolicy.AaStatTcaFilterCfg	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aaStatTcaFilterThrshCross	Release: • N/A
Description: The alarm is generated when the utilization matching a AaStatTcaFilterCfg in the past minute is greater than or equal to the value of tcaHighWatermark and the notification is not currently raised for the same entry.		
Remedial action: The utilization of the AA Statistics TCA Filter(s) which are configured in the AA Statistics TCA Filter Policy are equal or higher than the configured high watermark. Make an adjustment to the watermark.		

Table 39-6 AaStatTcaFltrEntryThrshCross

Alarm	Attributes	Applicable major release
Name: AaStatTcaFltrEntryThrshCross (9636) Type: processingErrorAlarm Package: aapolicy.AaStatTcaFltrEntryThrshCross Raised on class: aapolicy.AaStatTcaFltrEntryCfg	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aaStatTcaFltrEntryThrshCross	Release: • N/A

Table 39-6 AaStatTcaFltrEntryThrshCross (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is generated when the utilization matching a AaStatTcaFltrEntryCfg in the past minute is greater than or equal to the value of tcaHighWatermark and the notification is not currently raised for the same entry.		
Remedial action: The utilization of the AA Statistics TCA Filter Entry(Entries) which are configured in the AA Statistics TCA Entry Policy are equal or higher than the configured high watermark. Make an adjustment to the watermark.		

Table 39-7 AaStatTcaPolicerThrshCross

Alarm	Attributes	Applicable major release
Name: AaStatTcaPolicerThrshCross (9637) Type: processingErrorAlarm Package: aapolicy.AaStatTcaPolicerThrshCross Raised on class: aapolicy.AaStatTcaPolicerCfg	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aaStatTcaPolicerThrshCross	Release: • N/A
Description: The alarm is generated when the utilization matching a AaStatTcaPolicerCfg in the past minute is greater than or equal to the value of tcaHighWatermark and the notification is not currently raised for the same entry.		
Remedial action: The utilization of the AA Statistics TCA Policer(s) which are configured in the AA Statistics TCA Policer Policy are equal or higher than the configured high watermark. Make an adjustment to the watermark.		

Table 39-8 AaTcpValTcaCrossed

Alarm	Attributes	Applicable major release
Name: AaTcpValTcaCrossed (11057) Type: processingErrorAlarm Package: aapolicy.AaTcpValTcaCrossed Raised on class: aapolicy.AaTcpValidationTca	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aaTcpValTcaCrossed	Release: • N/A
Description: The alarm is generated when the utilization matching a tmnxBsxTcpValTcaEntry in the past minute is greater than or equal to the value of tmnxBsxTcpValTcaHighWatermark and the notification is not currently raised for the same entry.		
Remedial action: The utilization of the AA TCP Validation template(s) which are configured in the AA Statistics TCA Validation entry in the past minute is greater than or equal to the value of the high watermark. Make an adjustment to the watermark.		

Table 39-9 AAUrlFilterStateChanged

Alarm	Attributes	Applicable major release
Name: AAUrlFilterStateChanged (4972) Type: processingErrorAlarm Package: aapolicy.AAUrlFilterStateChanged Raised on class: aapolicy.AAUrlFilter	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: aAUrlFilterStateChanged	Release: • N/A
Description: The notification alarm is raised when the operational status has transitioned from 'In Service' to 'Out of Service' and cleared when operational status transitioned from 'Out of Service' to 'In Service'.		

Table 39-9 AAUrlFilterStateChanged (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Operational State' EQUAL 'Down') AND ('isLocal' EQUAL 'true'))		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Informational - This is a notification alarm to indicate that AA URL Filter which is configured in the AA URL Filter Policy is changing operational state.		

Table 39-10 ABSAlarm

Alarm	Attributes	Applicable major release
Name: ABSAlarm (5187) Type: equipmentAlarm Package: isa.ABSAlarm Raised on class: isa.MgGroupMember	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A
Description: The ABSAlarm is raised when a set of the internal parameters for ICC call latency and memory utilization reach the high threshold (activated) and cleared when it drop back and keep staying below the low threshold for at least some time period (de-activated)		
Remedial action: Diagnose why high memory utilization and/or control signaling overload happen.		

Table 39-11 AccountingPolicyDown

Alarm	Attributes	Applicable major release
Name: AccountingPolicyDown (538) Type: AccountingPolicy Package: accounting.AccountingPolicyDown Raised on class: accounting.Policy	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: accountingPolicyDown	Release: • N/A
Description: The alarm is raised when an accounting policy goes operationally Down after a file creation failure at the specified admin and backup locations.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: The file creation error is most likely a result of a flash disk full condition. Please analyse the content of the flash disk and remove redundant files. After this operation is complete please administratively toggle the accounting policy down/up. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-12 ActivationSessionActiveTooLong

Alarm	Attributes	Applicable major release
Name: ActivationSessionActiveTooLong (1153) Type: configurationAlarm Package: activation.ActivationSessionActiveTooLong Raised on class: activation.Session	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: activationSessionOpen	Release: • N/A
Description: The alarm is raised when an activation session has been active for a long time.		
Remedial action: Close the Activation Session.		

Table 39-13 ActivationSessionAutoClosed

Alarm	Attributes	Applicable major release
Name: ActivationSessionAutoClosed (12372) Type: configurationAlarm Package: activation.ActivationSessionAutoClosed Raised on class: activation.Session	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: activationSessionIdleTooLong	Release: • N/A
Description: The alarm is raised when an idle activation session is closed automatically.		
Remedial action: Informational - no corrective action required.		

Table 39-14 ActiveCPMMgmtEthernetPortDown

Alarm	Attributes	Applicable major release
Name: ActiveCPMMgmtEthernetPortDown (9572) Type: communicationsAlarm Package: netw.ActiveCPMMgmtEthernetPortDown Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ActiveCPMMgmtEthernetPort-Down	Release: • N/A
Description: The alarm is raised when the active CPM's management Ethernet port goes operationally down and the standby CPM's management Ethernet port is operationally up and now serving as the system's management Ethernet port.		
Remedial action: Active CPM's management Ethernet port goes operationally down and the standby CPM's management Ethernet port is operationally up and now serving as the system's management Ethernet port.		

Table 39-15 ActivitySwitch

Alarm	Attributes	Applicable major release
Name: ActivitySwitch (182) Type: communicationsAlarm Package: netw.ActivitySwitch Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: systemFailed	Release: • N/A

Table 39-15 ActivitySwitch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a 5620 SAM main server activity switch occurs.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why connectivity between the primary and standby SAM servers is unreliable.		

Table 39-16 AddressAttachFailed (service)

Alarm	Attributes	Applicable major release
Name: AddressAttachFailed (8134) Type: processingErrorAlarm Package: service.AddressAttachFailed Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: addressAttachFailed	Release: • N/A
Description: The alarm is raised when an IP address could not be attached to an interface.		
Remedial action: An IP address could not be attached to an interface. A possible cause is that a duplicate address is detected.		

Table 39-17 AddressAttachFailed (rtr)

Alarm	Attributes	Applicable major release
Name: AddressAttachFailed (8134) Type: processingErrorAlarm Package: rtr.AddressAttachFailed Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: addressAttachFailed	Release: • N/A
Description: The alarm is raised when an IP address could not be attached to an interface.		
Remedial action: An IP address could not be attached to an interface. A possible cause is that a duplicate address is detected.		

Table 39-18 AddressMisconfiguration

Alarm	Attributes	Applicable major release
Name: AddressMisconfiguration (591) Type: configurationAlarm Package: service.AddressMisconfiguration Raised on class: service.Service	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpipeBackboneMacAddressMismatch Applicable probable causes: • EpipeBackboneMacAddressMismatch • BVplsSourceMacAddressDuplicate	Release: • N/A

Table 39-18 AddressMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when B-VPLS site addresses are misconfigured. The EpipeBackboneMacAddressMismatch probable cause indicates that the backbone destination MAC address does not match the backbone source MAC address of the site on the destination NE. The BVplsSourceMacAddressDuplicate probable cause indicates that there are duplicate backbone source MAC addresses.		
Remedial action: Reconfigure the backbone MAC address so that the destination MAC address match the destination site for an EPIPE, or the source MAC address is not duplicate to the other source MAC address for a B-VPLS.		

Table 39-19 AdvNotActivated

Alarm	Attributes	Applicable major release
Name: AdvNotActivated (741) Type: configurationAlarm Package: vrrp.AdvNotActivated Raised on class: vrrp.InstanceV6	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: advertisementNotActivated	Release: • N/A
Description: The alarm is raised when the parent interface of an IPv6 VR instance is not configured to send router advertisements, or when router advertisement is not configured to use the virtual MAC address.		
Remedial action: Activate the Advertisement for the interface for the VRRP so that it sends Advertisement and Use Virtual MAC Address.		

Table 39-20 Ais

Alarm	Attributes	Applicable major release
Name: Ais (736) Type: communicationsAlarm Package: equipment.Ais Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ais	Release: • N/A
Description: The alarm is raised when an NE reports an AIS condition on the Tx or Rx circuit of a PDH tributary.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-21 AlarmDebouncingThresholdReached

Alarm	Attributes	Applicable major release
Name: AlarmDebouncingThresholdReached (11177) Type: communicationsAlarm Package: netw.AlarmDebouncingThresholdReached Raised on class: netw.NmsSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: debouncingCacheFull	Release: • N/A
Description: The alarm is raised when the cache that handles alarm debouncing is at capacity with excess bouncing alarms. When this happens, Alarm Debouncing is disabled and all alarm clear events that are being debounced are processed immediately. Alarm Debouncing is re-enabled after the processing of cached events completes.		

Table 39-21 AlarmDebouncingThresholdReached (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - Debounced alarms are being processed immediately to accommodate further bouncing alarms. If the problem persists, consider refining your alarm debouncing policy configurations or investigating why the network is generating so many bouncing alarms.		

Table 39-22 AlarmIndicationSignalOnHOPath

Alarm	Attributes	Applicable major release
Name: AlarmIndicationSignalOnHOPath (9005) Type: communicationsAlarm Package: tdm.AlarmIndicationSignalOnHOPath Raised on class: tdm.AUn	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AISP	Release: • N/A
Description: The alarm is raised on Alarm Indication Signal on HO Path (NEND).		
Remedial action: Alarm Indication Signal detected on HO Path (NEND).		

Table 39-23 AlarmQueueOverflowed

Alarm	Attributes	Applicable major release
Name: AlarmQueueOverflowed (3683) Type: qualityOfServiceAlarm Package: netw.AlarmQueueOverflowed Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: queueSizeExceeded	Release: • N/A
Description: The alarm is raised when the alarm queue size exceeds the allowed maximum. When this happens, the 5620 SAM discards alarms.		
Remedial action: An excessive number of traps are being received by 5620 SAM from the NEs in the network. 5620 SAM discards excess traps and recovers them from the network once the trap rate subsides. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-24 AlarmReplayFailure

Alarm	Attributes	Applicable major release
Name: AlarmReplayFailure (5121) Type: communicationsAlarm Package: netw.AlarmReplayFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: communicationsProtocolError	Release: • N/A
Description: The alarm is raised when the Alarm Replay fails. It is stored in Alarm Historical table.		
Remedial action: An Alarm Replay has failed (usually due to communication problems) - Some alarms may be missing in the Historical Alarm List.		

Table 39-25 AllArchiveLogsDeleted

Alarm	Attributes	Applicable major release
Name: AllArchiveLogsDeleted (199) Type: databaseAlarm Package: db.AllArchiveLogsDeleted Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: archivedLogsIssue	Release: • N/A
Description: The alarm is raised when the 5620 SAM deletes all database archive logs because it requires more disk space. When database disk space is low, the 5620 SAM first deletes the archive logs that have been applied to the standby database and raises the OldArchiveLogsDeleted alarm. If deleting the applied archive logs does not free up sufficient disk space, the 5620 SAM deletes the remaining archive logs, which creates an archive log gap that requires a standby database reinstantiation to correct. The alarm is raised only in a redundant 5620 SAM system.		
Remedial action: The standby database should be manually re-instantiated using the commands available in the SAM GUI. Please contact your Nokia support representative for further investigation.		

Table 39-26 AllBgpPeerConnectionsDown

Alarm	Attributes	Applicable major release
Name: AllBgpPeerConnectionsDown (5417) Type: topologyAlarm Package: topology.AllBgpPeerConnectionsDown Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPAAPeerConnectionDown	Release: • N/A
Description: The alarm is raised when all CPAA's BGP peers went down.		
Remedial action: 1) All BGP peer connections are down for the active CPAA. Please check the connections.\n2) If the standby CPAA is functional as per your requirements, switch-over might resolve the issue.		

Table 39-27 AllowInBandMismatchAlarm

Alarm	Attributes	Applicable major release
Name: AllowInBandMismatchAlarm (8419) Type: integrityViolation Package: gmpls.AllowInBandMismatchAlarm Raised on class: gmpls.DbLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: allowInBandMismatch	Release: • N/A
Description: The alarm is raised when the Allow In Band configured on the endpoints of the DB Link do not match.		
Remedial action: This alarm indicates that the allow in band property configured on the endpoints of the discovered DB Link do not match. Please make sure the allow in band is the same on the databearers at each end.		

Table 39-28 AllTimingReferencesNotQualified

Alarm	Attributes	Applicable major release
Name: AllTimingReferencesNotQualified (549) Type: communicationsAlarm Package: sonet.AllTimingReferencesNotQualified Raised on class: sonet.SiteSync	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: allTimingReferencesNotQualified	Release: • N/A
Description: The alarm is raised when no timing references on an NE are in the Qualified state.		
Raising condition: (('Qualified For Use' NOT EQUAL 'Qualified') AND ('Qualified For Use' NOT EQUAL 'Qualified') AND ('Qualified For Use' NOT EQUAL 'Qualified') AND ('Qualified For Use' NOT EQUAL 'Qualified'))		
Clearing condition: (('Qualified For Use' EQUAL 'Qualified') OR ('Qualified For Use' EQUAL 'Qualified') OR ('Qualified For Use' EQUAL 'Qualified') OR ('Qualified For Use' EQUAL 'Qualified'))		
Remedial action: Make sure that all the Timing References are qualified.		

Table 39-29 apsCfgRaiseAlarm

Alarm	Attributes	Applicable major release
Name: apsCfgRaiseAlarm (772) Type: configurationAlarm Package: ethernettunnel.apsCfgRaiseAlarm Raised on class: ethernettunnel.EthernetTunnelEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a mismatch between the working and protection Ethernet tunnel group configurations.		
Remedial action: Fix the mismatch between the working and protection Ethernet tunnel configurations.		

Table 39-30 apsNoRspRaiseAlarm

Alarm	Attributes	Applicable major release
Name: apsNoRspRaiseAlarm (773) Type: configurationAlarm Package: ethernettunnel.apsNoRspRaiseAlarm Raised on class: ethernettunnel.EthernetTunnelEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteProtectionSwitching	Release: • N/A
Description: The alarm is raised when an Ethernet tunnel group protection switch is incomplete, as indicated by a comparison of the transmitted 'Requested Signal' values and the received 'Bridged Signal' in the APS protocol.		
Remedial action: Fix the mismatch between the working and protection Ethernet tunnel configurations.		

Table 39-31 apsPrvsnAlarm

Alarm	Attributes	Applicable major release
Name: apsPrvsnAlarm (1196) Type: configurationAlarm Package: ethring.apsPrvsnAlarm Raised on class: ethring.Element	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: provisioningMismatch	Release: • N/A
Description: The alarm is raised when a mismatch is detected on Ethernet Ring provisioning. The mismatch occurs when the RPL Owner Node receives one or more No Request R-APS message(s) with an RPL blocked status flag set (NR, RB) and a different Node ID.		
Remedial action: Probably more than one Ring Protection Link owners configured in the Ring, make sure which one should be RPL owner and delete others.		

Table 39-32 apsPrvsnRaiseAlarm

Alarm	Attributes	Applicable major release
Name: apsPrvsnRaiseAlarm (774) Type: configurationAlarm Package: ethernettunnel.apsPrvsnRaiseAlarm Raised on class: ethernettunnel. EthernetTunnelEndpoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: provisioningMismatch	Release: • N/A
Description: The alarm is raised when an Ethernet tunnel group provisioning mismatch is detected at the ETH layer. The mismatch is detected through a comparison of the transmitted and received APS protocol A, B and D bits.		
Remedial action: Check the configuration of the two ends of the tunnel are compatible/same for the protocol.		

Table 39-33 APSSwitchover

Alarm	Attributes	Applicable major release
Name: APSSwitchover (8376) Type: equipmentAlarm Package: aps.APSSwitchover Raised on class: aps.ApsGroup	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: apsEventSwitchover	Release: • N/A
Description: The alarm is raised when APS Switchover happens either from the working channel to the protection or from the protection channel to the working.		
Remedial action: Informational - Make sure that the working/protection channel of the APS Group is up and operational.		

Table 39-34 ArchiveLogDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: ArchiveLogDiskSpaceBelowThreshold (197) Type: databaseAlarm Package: db.ArchiveLogDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary or standalone database archived log disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The archive log directory has become too full. Performing a manual database backup is required to reduce the size of this directory. If the alarm persists then the frequency of database backups must be increased.		

Table 39-35 ArchiveLogDiskSpaceSizeMisMatch

Alarm	Attributes	Applicable major release
Name: ArchiveLogDiskSpaceSizeMisMatch (2935) Type: diskSpaceIssue Package: db.ArchiveLogDiskSpaceSizeMisMatch Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary and standby database archived log directory sizes do not match.		
Remedial action: Disk space should be adjusted on the database servers to ensure adequate and equal space is reserved.		

Table 39-36 ArpEntriesExceededLimit (rtr)

Alarm	Attributes	Applicable major release
Name: ArpEntriesExceededLimit (9588) Type: communicationsAlarm Package: rtr.ArpEntriesExceededLimit Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ArpEntriesExceededLimit	Release: • N/A
Description: The alarm is raised when the number of IPv4 ARP entries learned on an IP interface has exceeded the configured maximum.		
Remedial action: Need to increase the ARP Limit since number of ARP entries have exceeded the configured limit so no new entries are learned until an entry expires.		

Table 39-37 ArpEntriesExceededLimit (service)

Alarm	Attributes	Applicable major release
Name: ArpEntriesExceededLimit (9588) Type: communicationsAlarm Package: service.ArpEntriesExceededLimit Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ArpEntriesExceededLimit	Release: • N/A

Table 39-37 ArpEntriesExceededLimit (service) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of IPv4 ARP entries learned on an IP interface has exceeded the configured maximum.		
Remedial action: Need to increase the ARP Limit since number of ARP entries have exceeded the configured limit so no new entries are learned until an entry expires.		

Table 39-38 ArpEntriesExceededThresholdLimit (rtr)

Alarm	Attributes	Applicable major release
Name: ArpEntriesExceededThresholdLimit (9589) Type: communicationsAlarm Package: rtr.ArpEntriesExceededThresholdLimit Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ArpEntriesExceededThresh-oldLimit	Release: • N/A
Description: The alarm is raised when the number of IPv4 ARP entries learned on an IP interface has exceeded vRtrIfArpThreshold percent of the configured maximum as specified by vRtrIfArpLimit.		
Remedial action: Need to increase the ARP Limit.		

Table 39-39 ArpEntriesExceededThresholdLimit (service)

Alarm	Attributes	Applicable major release
Name: ArpEntriesExceededThresholdLimit (9589) Type: communicationsAlarm Package: service.ArpEntriesExceededThresholdLimit Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ArpEntriesExceededThresh-oldLimit	Release: • N/A
Description: The alarm is raised when the number of IPv4 ARP entries learned on an IP interface has exceeded vRtrIfArpThreshold percent of the configured maximum as specified by vRtrIfArpLimit.		
Remedial action: Need to increase the ARP Limit.		

Table 39-40 ArpHostOverride

Alarm	Attributes	Applicable major release
Name: ArpHostOverride (9573) Type: processingErrorAlarm Package: netw.ArpHostOverride Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: arpHostOverride	Release: • N/A

Table 39-40 ArpHostOverride (continued)

Alarm	Attributes	Applicable major release
Description: The system generates an svcArpHostOverride notification when it overrides the MAC address of an ARP host. The new MAC address is in svcArpHostMacAddr, while the old MAC address is in svcNotifyMacAddress. [CAUSE] The system overrides the MAC address of an ARP host, because an ARP host with the same IP address as a known ARP host has appeared with a different MAC address. [EFFECT] The MAC address of the known ARP host has changed. [RECOVERY] No recovery required.		
Remedial action: Informational - no recovery needed.		

Table 39-41 AssuranceEventLoggingTurnedOff

Alarm	Attributes	Applicable major release
Name: AssuranceEventLoggingTurnedOff (9029) Type: processingErrorAlarm Package: assurance.AssuranceEventLoggingTurnedOff Raised on class: assurance.AssuranceEventManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: This alarm is raised when database disk space used to log Assurance Events grows above pre-defined threshold and the internal defense mechanism turns off Assurance Event logging to protect the database disk space.		
Remedial action: Purge Assurance Event records and wait until all of the alarms DatafileSizeAboveThreshold on EVENT_HISTORY files are cleared, then enable Assurance Event logging.		

Table 39-42 AsymmetricalConfig (bundle)

Alarm	Attributes	Applicable major release
Name: AsymmetricalConfig (295) Type: configurationAlarm Package: bundle.AsymmetricalConfig Raised on class: bundle.MultiChassisApsInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asymmetricalConfig	Release: • N/A
Description: The alarm is raised when the bundles in an APS group do not have matching configurations.		
Raising condition: ('Asymmetrical Config Detected' EQUAL 'true')		
Clearing condition: ('Asymmetrical Config Detected' EQUAL 'false')		
Remedial action: Check configurations on both members to see anything not matched.		

Table 39-43 ATPCHighPowerTimeout

Alarm	Attributes	Applicable major release
Name: ATPCHighPowerTimeout (4818) Type: communicationsAlarm Package: mwa.ATPCHighPowerTimeout Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ATPCLoopProblem	Release: • N/A

Table 39-43 ATPCHighPowerTimeout (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MPT detects a ATPC High Power Timeout		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-44 AuthenticationFailure

Alarm	Attributes	Applicable major release
Name: AuthenticationFailure (128) Type: communicationsAlarm Package: security.AuthenticationFailure Raised on class: security.TSecurityManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: multipleSecurityViolations	Release: • N/A
Description: The alarm is raised when a configurable number of attempts to log in to a 5620 SAM client fail. The alarm information includes the user name. The 5620 SAM will clear the alarm upon a successful user login or account deletion.		
Remedial action: Informational - the additional text field of the alarm will provide more details.		

Table 39-45 AuthFailure

Alarm	Attributes	Applicable major release
Name: AuthFailure (281) Type: authenticationAlarm Package: vrrp.AuthFailure Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authFailure	Release: • N/A
Description: The alarm is raised when authentication fails. The alarm information includes the source IP address.		
Remedial action: Reconfigure the authentication key so that the keys are the same for the peer VRRP instances.		

Table 39-46 AuthKeyConflict (ldp)

Alarm	Attributes	Applicable major release
Name: AuthKeyConflict (5188) Type: processingErrorAlarm Package: ldp.AuthKeyConflict Raised on class: ldp.Peer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • N/A
Description: The alarm is raised when both Authentication Key and LDP Peer Keychain are configured. LDP Peer Keychain will be used.		
Remedial action: Authentication Key and LDP Peer Keychain are both configured. LDP Peer Keychain will be used. The alarm is cleared when only one is configured.		

Table 39-47 AuthKeyFailure

Alarm	Attributes	Applicable major release
Name: AuthKeyFailure (8389) Type: processingErrorAlarm Package: ldp.AuthKeyFailure Raised on class: ldp.PeerTransport	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AuthKeyConflict	Release: • N/A
Description: The alarm is raised when both Authentication Key and LDP Peer Keychain are configured. LDP PeerTransport Keychain will be used.		
Remedial action: Authentication Key and LDP Peer Transport Keychain are both configured. LDP Peer Transport Keychain will be used. The alarm is cleared when only one is configured.		

Table 39-48 AuthorizationFailure

Alarm	Attributes	Applicable major release
Name: AuthorizationFailure (529) Type: communicationsAlarm Package: security.AuthorizationFailure Raised on class: security.TSecurityManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: multipleSecurityViolations	Release: • N/A
Description: The alarm is raised when a configurable number of attempts to delete or modify an object that is not in the current user span of control fail.		
Remedial action: Informational - the additional text field of the alarm will provide more details.		

Table 39-49 AuxDatabaseBackupFailed

Alarm	Attributes	Applicable major release
Name: AuxDatabaseBackupFailed (9613) Type: configurationAlarm Package: db.AuxDatabaseBackupFailed Raised on class: db.AuxiliaryDbBackup	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: databaseBackupFailure	Release: • N/A
Description: The alarm is raised when the auxiliary database backup files cannot be created because of, for example, a lack of disk space or insufficient file permissions.		
Raising condition: ('Latest Backup State' EQUAL 'Failed')		
Remedial action: Check the additional text of the alarm for guidance as to the specifics of the problem. Possible causes are lack of disk space or insufficient file permissions or the backup cannot finish on time. If the backup cannot finish on time, re-attempt the database backup.		

Table 39-50 AuxDbCannotRollbackToLastGoodEpoch

Alarm	Attributes	Applicable major release
Name: AuxDbCannotRollbackToLastGoodEpoch (9638) Type: databaseAlarm Package: db.AuxDbCannotRollbackToLastGoodEpoch Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: This informative alarm is raised when the auxiliary database is corrupted and cannot be started nor rolled back to the last good epoch.		
Remedial action: The auxiliary database is corrupted and cannot be started nor rolled back to the last good epoch. Statistics collection is stopped. Please contact your Nokia support representative.		

Table 39-51 AuxDbCannotStart

Alarm	Attributes	Applicable major release
Name: AuxDbCannotStart (10271) Type: databaseAlarm Package: db.AuxDbCannotStart Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: This informative alarm is raised when the auxiliary database cannot be automatically started.		
Remedial action: The auxiliary database cannot be started automatically. Statistics collection is stopped. Please contact your Nokia support representative.		

Table 39-52 AuxiliaryAlarm

Alarm	Attributes	Applicable major release
Name: AuxiliaryAlarm (1159) Type: dryContactAlarm Package: equipment.AuxiliaryAlarm Raised on class: equipment.AuxAlarmDefinition	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: auxliaryAlarmTriggered	Release: • N/A
Description: The alarm is raised when an NE reports that a configured auxiliary alarm condition has been triggered.		
Remedial action: Informational - no corrective action required.		

Table 39-53 AuxiliaryDatabaseClusterUnavailable

Alarm	Attributes	Applicable major release
Name: AuxiliaryDatabaseClusterUnavailable (8154) Type: databaseAlarm Package: db.AuxiliaryDatabaseClusterUnavailable Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A

Table 39-53 AuxiliaryDatabaseClusterUnavailable (continued)

Alarm	Attributes	Applicable major release
Description: This informative alarm is raised when the auxiliary database cluster is not available.		
Remedial action: The auxiliary database cluster is not responding. This means all the nodes in the cluster are down. Stats collection is stopped. Please restart the auxiliary database cluster.		

Table 39-54 AuxiliaryDatabaseConnectivityStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryDatabaseConnectivityStatus (9614) Type: communicationsAlarm Package: db.AuxiliaryDatabaseConnectivityStatus Raised on class: db.AuxiliaryDatabase	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: This informative alarm is raised when a 5620 SAM server cannot communicate with an auxiliary database server. The alarm clears when communication is restored.		
Raising condition: ('Connectivity State' EQUAL 'Offline')		
Clearing condition: ('Connectivity State' EQUAL 'Online')		
Remedial action: The 5620 SAM server is unable to communicate with an auxiliary database. Check the status of the auxiliary database and the communication link between SAM server and auxiliary database node.		

Table 39-55 AuxiliaryDatabaseNodeFailed

Alarm	Attributes	Applicable major release
Name: AuxiliaryDatabaseNodeFailed (9615) Type: databaseAlarm Package: db.AuxiliaryDatabaseNodeFailed Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: This informative alarm is raised when the auxiliary database node failed and was stopped.		
Remedial action: The auxiliary database node failed and was stopped. Please fix the issue with the auxiliary database node and re-start the auxiliary database process.		

Table 39-56 AuxiliaryDatabaseStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryDatabaseStatus (5173) Type: communicationsAlarm Package: db.AuxiliaryDatabaseStatus Raised on class: db.AuxiliaryDatabase	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A

Table 39-56 AuxiliaryDatabaseStatus (continued)

Alarm	Attributes	Applicable major release
Description: This informative alarm is raised when a 5620 SAM server detects that an auxiliary database server is down. The alarm clears when the node is restored.		
Raising condition: ('State' EQUAL 'Down')		
Clearing condition: ('State' EQUAL 'Up')		
Remedial action: The 5620 SAM server detected an auxiliary database is down. Check the status of the auxiliary database.		

Table 39-57 AuxiliaryServerAssignmentProblem

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerAssignmentProblem (5135) Type: processingErrorAlarm Package: server.AuxiliaryServerAssignmentProblem Raised on class: server.AuxiliaryServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: This alarm is raised when a NE cannot be assigned to an AuxiliaryServer during load balancing or manual assignment operation.		
Remedial action: Ensure the NE is managed, reachable and that no configuration operation is in progress on that NE and relaunch the operation.		

Table 39-58 BackgroundDiagnosticFault

Alarm	Attributes	Applicable major release
Name: BackgroundDiagnosticFault (467) Type: equipmentAlarm Package: equipment.BackgroundDiagnosticFault Raised on class: equipment.ReplaceableUnit	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backgroundDiagnosticFault	Release: • N/A
Description: The alarm is raised when an NE detects a failure in a background diagnostic test suite.		
Remedial action: Informational - if the condition persists then the element indicated in the alarm should be replaced.		

Table 39-59 backhaulServiceDown

Alarm	Attributes	Applicable major release
Name: backhaulServiceDown (11463) Type: communicationsAlarm Package: mpr.backhaulServiceDown Raised on class: mpr.BackhaulService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: backhaulServiceDown	Release: • N/A
Description: The alarm is raised when the service is down.		

Table 39-59 backhaulServiceDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL '3')		
Clearing condition: ('Operational State' EQUAL '1')		
Remedial action: Check any affected adjancency/Site.		

Table 39-60 BackupDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: BackupDiskSpaceBelowThreshold (195) Type: databaseAlarm Package: db.BackupDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary or standalone database backup disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The additional text field of the alarm will provide more details. Additional disk space must be made available for the backup location or a different, larger backup location must be configured.		

Table 39-61 BatteryFail (equipment)

Alarm	Attributes	Applicable major release
Name: BatteryFail (616) Type: equipmentAlarm Package: equipment.BatteryFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: batteryFail	Release: • N/A
Description: The alarm is raised when the battery fails or is missing.		
Remedial action: The battery on the CPM should be replaced or re-installed.		

Table 39-62 BfdSessionDown (service)

Alarm	Attributes	Applicable major release
Name: BfdSessionDown (439) Type: bfdSessionAlarm Package: service.BfdSessionDown Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • N/A
Description: The alarm is raised when a BFD session is operationally down.		

Table 39-62 BfdSessionDown (service) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when a BFD session on a L3 access interface goes down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-63 BfdSessionDown (vprn)

Alarm	Attributes	Applicable major release
Name: BfdSessionDown (439) Type: bfdSessionAlarm Package: vprn.BfdSessionDown Raised on class: vprn.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • N/A
Description: The alarm is raised when a BFD session is operationally Down.		
Remedial action: This alarm is raised when a BFD session on a VPRN network interface goes down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-64 BfdSessionDown (rtr)

Alarm	Attributes	Applicable major release
Name: BfdSessionDown (439) Type: bfdSessionAlarm Package: rtr.BfdSessionDown Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • N/A
Description: The alarm is raised when a BFD session is operationally down.		
Remedial action: This alarm is raised when a BFD session on a network interface goes down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-65 BfdSessionFlapped (rtr)

Alarm	Attributes	Applicable major release
Name: BfdSessionFlapped (3900) Type: bfdSessionAlarm Package: rtr.BfdSessionFlapped Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: bfdSessionFlapped	Release: • N/A

Table 39-65 BfdSessionFlapped (rtr) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a BFD session transitions from Up to Down and back to Up within the BFD operational state transition interval.		
Remedial action: The BFD session on a network interface has transitioned from Up to Down and back to Up within the configured BFD Flapping Interval.		

Table 39-66 BfdSessionFlapped (service)

Alarm	Attributes	Applicable major release
Name: BfdSessionFlapped (3900) Type: bfdSessionAlarm Package: service.BfdSessionFlapped Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionFlapped	Release: • N/A
Description: The alarm is raised when a BFD session transitions from Up to Down and back to Up within the BFD operational state transition interval.		
Remedial action: The BFD session on a L3 access interface has transitioned from Up to Down and back to Up within the configured BFD Flapping Interval.		

Table 39-67 BfdSessionFlapped (vprn)

Alarm	Attributes	Applicable major release
Name: BfdSessionFlapped (3900) Type: bfdSessionAlarm Package: vprn.BfdSessionFlapped Raised on class: vprn.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionFlapped	Release: • N/A
Description: The alarm is raised when a BFD session transitions from Up to Down and back to Up within the BFD operational state transition interval.		
Remedial action: The BFD session on a VPRN network interface has transitioned from Up to Down and back to Up within the configured BFD Flapping Interval.		

Table 39-68 BfdSessionMissing (service)

Alarm	Attributes	Applicable major release
Name: BfdSessionMissing (438) Type: bfdSessionAlarm Package: service.BfdSessionMissing Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionMissing	Release: • N/A
Description: The alarm is raised when a previously present BFD session is absent.		

Table 39-68 BfdSessionMissing (service) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when a previously present BFD session on a L3 access interface is absent. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the near end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-69 BfdSessionMissing (rtr)

Alarm	Attributes	Applicable major release
Name: BfdSessionMissing (438) Type: bfdSessionAlarm Package: rtr.BfdSessionMissing Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionMissing	Release: • N/A
Description: The alarm is raised when a previously present BFD session is absent.		
Remedial action: This alarm is raised when a previously present BFD session on a network interface is absent. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the near end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-70 BfdSessionMissing (vprn)

Alarm	Attributes	Applicable major release
Name: BfdSessionMissing (438) Type: bfdSessionAlarm Package: vprn.BfdSessionMissing Raised on class: vprn.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionMissing	Release: • N/A
Description: The alarm is raised when a previously present BFD session is absent.		
Remedial action: This alarm is raised when a previously present BFD session on a VPRN network interface is absent. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the near end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-71 BgpAdVplsIdDiscoveryError

Alarm	Attributes	Applicable major release
Name: BgpAdVplsIdDiscoveryError (572) Type: serviceAlarm Package: vpls.BgpAdVplsIdDiscoveryError Raised on class: vpls.AbstractSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bgpAdVplsIdInconsistent	Release: • N/A
Description: The alarm is raised when the VPLS ID of a discovered VPLS instance is ambiguous.		

Table 39-71 BgpAdVplsIdDiscoveryError (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check that all VPLS IDs are properly configured for all VPLS instances.		

Table 39-72 BgpAdVplsIdMisconfiguration

Alarm	Attributes	Applicable major release
Name: BgpAdVplsIdMisconfiguration (570) Type: configurationAlarm Package: vpls.BgpAdVplsIdMisconfiguration Raised on class: vpls.AbstractVpls	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bgpAdVplsIdInconsistent	Release: • N/A
Description: The alarm is raised when the VPLS ID of a site does not match the VPLS ID of the other sites in the service.		
Remedial action: All VPLS IDs of sites in a service must be the same.		

Table 39-73 BgpAsPathLenPerMonPrefThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpAsPathLenPerMonPrefThresholdReached (795) Type: topologyAlarm Package: topology. BgpAsPathLenPerMonPrefThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: asPathTooLong	Release: • N/A
Description: The alarm is raised when the AS path length for a monitored BGP route reaches or exceeds the maximum threshold value.		
Remedial action: User configured alarm for monitoring purpose. Alarm text provides information about the affected prefix. User can look at the records for BGP prefix monitoring or BGP events history for debugging purpose.		

Table 39-74 BgpEventDbSizeThresholdExceeded

Alarm	Attributes	Applicable major release
Name: BgpEventDbSizeThresholdExceeded (3703) Type: configurationAlarm Package: topology. BgpEventDbSizeThresholdExceeded Raised on class: topology.BgpEventPartitionManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BGPEventDBSizeIsNotSuffi-cient	Release: • N/A
Description: The alarm is raised when the actual DB size consumed by BGP Events exceeds the threshold.		
Remedial action: BGP Events DB storage reached threshold or exceeded, increase "Max BGP Events DB Size" in BGP Event Manager GUI.		

Table 39-75 BgpEventUnreachable

Alarm	Attributes	Applicable major release
Name: BgpEventUnreachable (4896) Type: topologyAlarm Package: topology.BgpEventUnreachable Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: prefixUnreachable	Release: • N/A
Description: The alarm is raised when Unreachable BGP Event is detected.		
Remedial action: Alarm text provides information about the affected prefix. User can look at the BGP events history for debugging purpose.		

Table 39-76 BgpFlowspecNlriProblem

Alarm	Attributes	Applicable major release
Name: BgpFlowspecNlriProblem (3317) Type: ProtocolAlarm Package: rtr.BgpFlowspecNlriProblem Raised on class: rtr.RoutingInstanceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NlriProblem	Release: • N/A
Description: The alarm is raised when the filter module receives a BGP FlowSpec NLRI that cannot be treated.		
Remedial action: Information - if the the problem persists please contact your Nokia support representative for assistance.		

Table 39-77 BgpMonitorPrefixFlapRateThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpMonitorPrefixFlapRateThresholdReached (432) Type: topologyAlarm Package: topology. BgpMonitorPrefixFlapRateThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstablePrefix	Release: • N/A
Description: The alarm is raised when a BGP monitor prefix flap rate exceeds the maximum flap rate threshold value.		
Remedial action: User configured alarm for monitoring purpose. Alarm text provides information about the affected prefix. User can look at the records for BGP prefix monitoring or BGP events history for debugging purpose.		

Table 39-78 BgpMonPrefixUnreachable

Alarm	Attributes	Applicable major release
Name: BgpMonPrefixUnreachable (1114) Type: topologyAlarm Package: topology.BgpMonPrefixUnreachable Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: prefixUnreachable	Release: • N/A

Table 39-78 BgpMonPrefixUnreachable (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when no route for the monitored prefix is detected.		
Remedial action: User configured alarm for monitoring purpose. Alarm text provides information about the affected prefix. User can look at the records for BGP prefix monitoring or BGP events history for debugging purpose.		

Table 39-79 BgpMonPrefRedundancyLossThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpMonPrefRedundancy-LossThresholdReached (796) Type: topologyAlarm Package: topology.BgpMonPrefRedundancyLossThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lowNumberofNHops	Release: • N/A
Description: The alarm is raised when the number of next hops for a monitored BGP route reaches or falls below the minimum threshold value.		
Remedial action: User configured alarm for monitoring purpose. Alarm text provides information about the affected prefix. User can look at the records for BGP prefix monitoring or BGP events history for debugging purpose.		

Table 39-80 BgpPktRateThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpPktRateThresholdReached (431) Type: topologyAlarm Package: topology.BgpPktRateThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableBgpSpeaker	Release: • N/A
Description: The alarm is raised when a BGP packet rate exceeds the maximum threshold value.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-81 BgpProfilePrefixUnreachable

Alarm	Attributes	Applicable major release
Name: BgpProfilePrefixUnreachable (8148) Type: topologyAlarm Package: topology.BgpProfilePrefixUnreachable Raised on class: topology.AbstractBgpRouteProfile	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: BGPProfilePrefixUnreachable	Release: • N/A
Description: The alarm is raised when the prefix on BGP profile is unreachable.		
Remedial action: BGP Profile matched with BGP prefix unreachable event.		

Table 39-82 BgpRouteChangeThresholdPerNHopReached

Alarm	Attributes	Applicable major release
Name: BgpRouteChangeThresholdPerNHopReached (601) Type: topologyAlarm Package: topology.BgpRouteChangeThresholdPerNHopReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableBgpSpeaker	Release: • N/A
Description: The alarm is raised when the number of BGP route changes for a next hop reaches the maximum threshold value for a next hop.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-83 BgpRouteChangeThresholdPerRTargetReached

Alarm	Attributes	Applicable major release
Name: BgpRouteChangeThresholdPer-RTargetReached (600) Type: topologyAlarm Package: topology.BgpRouteChangeThresholdPerRTargetReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableVpnSite	Release: • N/A
Description: The alarm is raised when the number of BGP route changes for a route target reaches the maximum threshold value for route targets.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-84 BgpRouteCountThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpRouteCountThresholdReached (428) Type: topologyAlarm Package: topology.BgpRouteCountThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyBgpRoute-ForNextHop	Release: • N/A
Description: The alarm is raised when the BGP route count for a next hop exceeds the maximum threshold value for next hops.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-85 BgpRouteFlapRateThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpRouteFlapRateThresholdReached (430) Type: topologyAlarm Package: topology. BgpRouteFlapRateThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableBgpSpeaker	Release: • N/A
Description: The alarm is raised when the BGP route flap rate exceeds the maximum threshold value.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-86 BgpRouteHighWatermarkPerRTargetReached

Alarm	Attributes	Applicable major release
Name: BgpRouteHighWatermarkPerRTargetReached (433) Type: topologyAlarm Package: topology. BgpRouteHighWatermarkPerRTargetReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyBgpRouteForGiven-RouteTarget	Release: • N/A
Description: The alarm is raised when there are too many BGP routes for a route target.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-87 BgpRouteLowWatermarkPerRTargetReached

Alarm	Attributes	Applicable major release
Name: BgpRouteLowWatermarkPerRTargetReached (434) Type: topologyAlarm Package: topology. BgpRouteLowWatermarkPerRTargetReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooLittleBgpRouteForGiven-RouteTarget	Release: • N/A
Description: The alarm is raised when there are too few BGP routes for a route target.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-88 BgpRouteRateThresholdPerRTargetReached

Alarm	Attributes	Applicable major release
Name: BgpRouteRateThresholdPerRTargetReached (435) Type: topologyAlarm Package: topology.BgpRouteRateThresholdPerRTargetReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableVpnSite	Release: • N/A
Description: The alarm is raised when the BGP route rate for a target reaches the maximum threshold value for route targets.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-89 BgpRouteRateThresholdReached

Alarm	Attributes	Applicable major release
Name: BgpRouteRateThresholdReached (429) Type: topologyAlarm Package: topology.BgpRouteRateThresholdReached Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyBgpRoute-ForNextHop	Release: • N/A
Description: The alarm is raised when the BGP route rate for a next hop exceeds the maximum threshold value for next hops.		
Remedial action: User configured alarm for monitoring purpose. BGP events history can be used for debugging purpose.		

Table 39-90 BidirectionalTPLspDestinationMisconfiguration

Alarm	Attributes	Applicable major release
Name: BidirectionalTPLspDestinationMisconfiguration (5117) Type: configurationAlarm Package: mplstp.BidirectionalTPLspDestinationMisconfiguration Raised on class: mplstp.GlobalTPLsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DestinationParametersMis-match	Release: • N/A
Description: The alarm is raised when the Destination Global ID, Destination Node ID, or Destination Tunnel Number is not consistent with the configuration of the opposite TP-LSP in a Bidirectional TP-LSP.		
Remedial action: This alarm is generated when a TP-LSP that belongs to a Bidirectional TP-LSP has any of its Destination Global ID, Destination Node ID, or Destination Tunnel Number misconfigured. Review the configuration both TP-LSPs in the Bidirectional TP-LSP and ensure that the Destination Global ID, Destination Node ID, and Destination Tunnel Number are configured properly.		

Table 39-91 BidirectionalTPLspPathLspNumberMisconfiguration

Alarm	Attributes	Applicable major release
Name: BidirectionalTPLspPathLspNum-berMisconfiguration (5118) Type: configurationAlarm Package: mplstp.BidirectionalTPLspPathLspNumberMisconfiguration Raised on class: mplstp.GlobalTPLspPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LSPNumberMismatch	Release: • N/A
Description: The alarm is raised when the LSP Path Number is not consistent with the LSP Path Number for LER A and LER B.		
Remedial action: This alarm is generated when the LSP Path Number for the Bidirectional TP-LSP Path does not match LER A and/or LER B. Review the configuration of LSP Path Number LER A and LER B and ensure both are set to the same value as the Bidirectional TP-LSP Path's LSP Path Number.		

Table 39-92 BidirIpPathMonitorPathsDiverge

Alarm	Attributes	Applicable major release
Name: BidirIpPathMonitorPathsDiverge (603) Type: topologyAlarm Package: monpath.BidirIpPathMonitorPathsDiverge Raised on class: monpath.BidirMonitoredIpPath	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipPathsDiverge	Release: • N/A
Description: The alarm is raised when the 5650 CPAM detects that the IP paths of a bidirectional IP path monitor diverge. The alarm clears when the paths converge. This may occur when an IP path monitor cannot be set up after the number of attempts specified by the cpamManagedRoute problematicThresholdAlarmAfter value in the nms-server.xml file. The alarm is raised if the cpamMan-agedRoute problematicRetryStrategy value in nms-server.xml is set to countdown. The default problematicRetryStrategy value of reactive prevents the alarm from being raised.		
Remedial action: Informational - Paths in both direction can be highlighted on the CPAM map to identify the divergence point.		

Table 39-93 BidirLspMonitorPathsDiverge

Alarm	Attributes	Applicable major release
Name: BidirLspMonitorPathsDiverge (1915) Type: topologyAlarm Package: monpath.BidirLspMonitorPathsDiverge Raised on class: monpath.BidirMonitoredLspPath	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LspPathsDiverge	Release: • N/A
Description: The alarm is raised when the LSP's active path's hops do not match in the forward and reverse direction.		
Remedial action: Informational - Paths in both direction can be highlighted on the CPAM map to identify the divergence point.		

Table 39-94 BITSReferenceLossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: equipment.BITSReferenceLossOfSignal Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • N/A
Description: The alarm is raised when the BITS Port reference on the Standby CPM is not qualified due to Loss of Signal.		
Remedial action: Make sure that peer connected to BITS Port on the Standby CPM is properly configured.		

Table 39-95 BITSReferenceOutOfFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: equipment.BITSReferenceOutOfFrequency Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • N/A
Description: The alarm is raised when the BITS Port reference on the Standby CPM is not qualified due to Out of frequency.		
Remedial action: Make sure that frequency configured for the BITS Port on the Standby CPM is correct.		

Table 39-96 BITSReferenceOutOfPollInRange (equipment)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: equipment.BITSReferenceOutOfPollInRange Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • N/A
Description: The alarm is raised when the BITS Port reference on the Standby CPM is not qualified due to Out of poll in range.		
Remedial action: Check the BITS Port on the Standby CPM is configured correctly and the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 39-97 BofSaveFailed

Alarm	Attributes	Applicable major release
Name: BofSaveFailed (11056) Type: equipmentAlarm Package: sw.BofSaveFailed Raised on class: sw.SoftwareUpgradeManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bofSaveFailed	Release: • N/A

Table 39-97 BofSaveFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the bof save failed		
Remedial action: Please log into the NE in question via CLI and execute a manual bof save. If the problem persists please contact Nokia support for assistance.		

Table 39-98 BootConfigFailScriptNotAccesible

Alarm	Attributes	Applicable major release
Name: BootConfigFailScriptNotAccesible (543) Type: configurationAlarm Package: netw.BootConfigFailScriptNotAccesible Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: bootConfigFailScriptNotAccesible	Release: • N/A
Description: The alarm is raised when a CLI script that runs after NE configuration file execution failure is inaccessible.		
Remedial action: Ensure that the CLI script (boot-bad-exec) that runs after an NE configuration file execution failure is accessible. The script location is configurable through CLI on the NE (configure system boot-bad-exec)		

Table 39-99 BootConfigOKScriptNotAccesible

Alarm	Attributes	Applicable major release
Name: BootConfigOKScriptNotAccesible (544) Type: configurationAlarm Package: netw.BootConfigOKScriptNotAccesible Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: bootConfigOKScriptNotAccesible	Release: • N/A
Description: The alarm is raised when a CLI script that runs after NE configuration file execution success is inaccessible.		
Remedial action: Ensure that the CLI script (boot-good-exec) file that runs after an NE configuration file execution success is accessible. The script location is configurable through CLI on the NE (configure system boot-good-exec)		

Table 39-100 BootEnvironmentSyncFailed

Alarm	Attributes	Applicable major release
Name: BootEnvironmentSyncFailed (101) Type: equipmentAlarm Package: sw.BootEnvironmentSyncFailed Raised on class: sw.SoftwareUpgradeManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootEnvironmentSyncFailed	Release: • N/A
Description: The alarm is raised when the synchronization of one or more system initialization files between the active and standby CPM cards fails, or when one or both of the CSM compact flash devices do not have enough space when the 'admin redundancy synchronize boot-env' command is executed, or when the node is rebooted.		

Table 39-100 BootEnvironmentSyncFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operator should make sure that the Boot Environment files on the CSM cards are in Sync with each other or there is enough space available on the compact flash.		

Table 39-101 BootLoaderFirmwareMismatchAlarm

Alarm	Attributes	Applicable major release
Name: BootLoaderFirmwareMismatchAlarm (617) Type: firmwareAlarm Package: equipment. BootLoaderFirmwareMismatchAlarm Raised on class: equipment.ControlProcessor	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: bootLoaderVersionMismatch	Release: • N/A
Description: The alarm is raised when there is a mismatch between the firmware version and the software image on an NE. The alarm information includes the discovered and expected version identifiers.		
Remedial action: Either the firmware or the device SW must be upgraded to compatible versions. The image (firmware or device SW) which is the oldest should be upgraded. Firmware must be upgraded using the NE's CLI. 5620 SAM can be used to upgrade the SW image on the device.		

Table 39-102 BootLoaderUpdateFailed

Alarm	Attributes	Applicable major release
Name: BootLoaderUpdateFailed (9017) Type: equipmentAlarm Package: sw.BootLoaderUpdateFailed Raised on class: sw.SoftwareUpgradeManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootLoaderUpdateFailed	Release: • N/A
Description: The alarm is raised when boot-loader update fails.		
Remedial action: The alarm is raised when boot-loader update fails. Investigate the cause of the failure and reattempt the update. If the problem persists contact your Nokia support representative for assistance.		

Table 39-103 BrokenLoop

Alarm	Attributes	Applicable major release
Name: BrokenLoop (469) Type: configurationAlarm Package: equipment.BrokenLoop Raised on class: equipment.StackConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: stackNotInLoop	Release: • N/A
Description: The alarm is raised when the loop-detection stack detects a loop condition, or when the stack contains an unexpected element.		
Remedial action: Login to switch console, check and correct configuration and reload stack.		

Table 39-104 BTSSoftwareResynchronization

Alarm	Attributes	Applicable major release
Name: BTSSoftwareResynchronization (11806) Type: configurationAlarm Package: sw.BTSSoftwareResynchronization Raised on class: sw.SoftwareUpgradeManager	Severity: major Specific problem: BTS Software Upgrade Failure. Implicitly cleared: true Default probable cause: FILE_ERROR	Release: • N/A
Description: The alarm is raised when an automatic NE software resynchronization initiated by the BTS failed. The detail of the error is set in the additional information of the alarm and in the resynchronization detail error of the BTS software upgrade status.		
Remedial action: Investigation is required to resolve the following possible scenarios: the BTS or OMS is unreachable (including underlying transport network issue); loss of connectivity to the BTS or OMS during transfer; CORBA and HTTP security credential issues.		

Table 39-105 BTSSoftwareUpgrade

Alarm	Attributes	Applicable major release
Name: BTSSoftwareUpgrade (11807) Type: configurationAlarm Package: sw.BTSSoftwareUpgrade Raised on class: sw.SoftwareUpgradeManager	Severity: major Specific problem: BTS Software Upgrade Failure. Implicitly cleared: true Default probable cause: FILE_ERROR	Release: • N/A
Description: The alarm is raised when an automatic NE software upgrade initiated by the BTS failed. The detail of the error is set in the additional information of the alarm and in the upgrade detail error of the BTS software upgrade status.		
Remedial action: Investigation is required to resolve the following possible scenarios: the BTS or LTE OMS is unreachable (including underlying transport network issue); loss of connectivity to the BTS or LTE OMS during transfer; CORBA and HTTP security credential issues; BTS software load is missing in SAM.		

Table 39-106 BWUtilizationExceeded

Alarm	Attributes	Applicable major release
Name: BWUtilizationExceeded (811) Type: thresholdCrossed Package: netw.BWUtilizationExceeded Raised on class: netw.AbstractPhysicalLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when the per-CoS or overall bandwidth utilization exceeds the configured threshold.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand how this Physical Link became overbooked		

Table 39-107 CacheSyncCommunicationFailure

Alarm	Attributes	Applicable major release
Name: CacheSyncCommunicationFailure (4390) Type: communicationsAlarm Package: server.CacheSyncCommunicationFailure Raised on class: server.SamServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectionEstablishmentError	Release: • N/A
Description: The alarm is raised when the 5620 SAM standby server cannot establish a warm redundancy connection with the 5620 SAM primary server.		
Remedial action: Please ensure the primary and standby servers are up and verify the cache-sync connection settings in nms-server.xml.		

Table 39-108 CAProfileStateChange

Alarm	Attributes	Applicable major release
Name: CAProfileStateChange (3910) Type: configurationAlarm Package: sitesec.CAProfileStateChange Raised on class: sitesec.CertificateAuthProfile	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: caProfileStateDown	Release: • N/A
Description: The alarm is raised when Certificate Authority profile changes state to 'down' due to tmnxSecNotifFailureReason.		
Remedial action: The Certificate Authority profile changes state to 'down'. Depending on the reason specified, corrective action should be taken		

Table 39-109 CAProfileUpDueToRevokeChkCrlOpt

Alarm	Attributes	Applicable major release
Name: CAProfileUpDueToRevokeChkCrlOpt (8417) Type: configurationAlarm Package: sitesec.CAProfileUpDueToRevokeChkCrlOpt Raised on class: sitesec.CertificateAuthProfile	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CAProfileUpDueToRevokeChkCrlOpt	Release: • N/A
Description: This alarm is raised when Certificate Authority profile state changes to 'up' even when there are other alarms, due to revocationCheck is set to 'crlOptional'.		
Remedial action: Certificate Authority profile will remain up but the other alarms on the Certificate Authority profile should still be corrected.		

Table 39-110 CardCPUAboveThreshold

Alarm	Attributes	Applicable major release
Name: CardCPUAboveThreshold (618) Type: configurationAlarm Package: equipment.CardCPUAboveThreshold Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CardCPUUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when the card CPU usage exceeds the threshold value.		
Remedial action: Informational - The CPU of the card indicated in the alarm is overloaded. If the condition persists then processing load should be transferred from this card to other cards which are more lightly loaded. If the problem persists then please contact your Nokia support representative for assistance.		

Table 39-111 CardMemoryAboveThreshold

Alarm	Attributes	Applicable major release
Name: CardMemoryAboveThreshold (619) Type: configurationAlarm Package: equipment.CardMemoryAboveThreshold Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CardMemoryUtilization-CrossedAboveThreshold	Release: • N/A
Description: The alarm is raised when the card memory usage exceeds the threshold value.		
Remedial action: Informational - The memory of the card indicated in the alarm is over utilized. If the condition persists then processing load should be transferred from this card to other cards which are more lightly loaded in order to reduce memory consumption. If the problem persists then please contact your Nokia support representative for assistance.		

Table 39-112 CardRxAboveThreshold

Alarm	Attributes	Applicable major release
Name: CardRxAboveThreshold (620) Type: configurationAlarm Package: equipment.CardRxAboveThreshold Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardRxUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when the card Rx exceeds the threshold value.		
Remedial action: The utilization of the card is higher than normal. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-113 CardRxTxAboveThreshold

Alarm	Attributes	Applicable major release
Name: CardRxTxAboveThreshold (621) Type: configurationAlarm Package: equipment.CardRxTxAboveThreshold Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardRxTxUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when the card Tx exceeds the threshold value.		
Remedial action: The utilization of the card is higher than normal. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-114 CardUnseated

Alarm	Attributes	Applicable major release
Name: CardUnseated (1161) Type: equipmentAlarm Package: equipment.CardUnseated Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CardUnseated	Release: • N/A
Description: The alarm is raised when a card is removed.		
Remedial action: Informational - no corrective action required.		

Table 39-115 CeAddressIncompatible

Alarm	Attributes	Applicable major release
Name: CeAddressIncompatible (251) Type: configurationAlarm Package: ipipe.CeAddressIncompatible Raised on class: ipipe.Ipipe	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ceAddressIncompatible	Release: • N/A
Description: The alarm is raised when two SAPs in an Ipipe have the same CE IP address, or when the CE IP address is not the same as the CE IP address of the peer SDP binding.		
Raising condition: ('ceAddressIncompatible' EQUAL 'true')		
Clearing condition: ('ceAddressIncompatible' EQUAL 'false')		
Remedial action: Modify the CE Address so that it's not same address as other SAPs and it matches the address of the peer SDP binding.		

Table 39-116 CertAfterExpWarning

Alarm	Attributes	Applicable major release
Name: CertAfterExpWarning (9601) Type: communicationsAlarm Package: sitesec.CertAfterExpWarning Raised on class: sitesec.CertificateAuthProfile	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: certAfterExpWarning	Release: • N/A
Description: The alarm is raised when the certificate file indicated in Certificate Authority profile is expired.		
Remedial action: Replace the indicated file with an updated certificate.		

Table 39-117 CertBeforeExpWarning

Alarm	Attributes	Applicable major release
Name: CertBeforeExpWarning (9602) Type: communicationsAlarm Package: sitesec.CertBeforeExpWarning Raised on class: sitesec.CertificateAuthProfile	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: certBeforeExpWarning	Release: • N/A
Description: The alarm is raised when the certificate file indicated in Certificate Authority profile will expire in the time period as indicated.		
Remedial action: Replace the indicated file with an updated certificate.		

Table 39-118 certifyFailureAlarm

Alarm	Attributes	Applicable major release
Name: certifyFailureAlarm (533) Type: softwareAlarm Package: sw.certifyFailureAlarm Raised on class: sw.SoftwareControlModule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: certifyFailureAlarm	Release: • N/A
Description: The alarm is raised when the software certification process on an NE fails.		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 39-119 CheckpointLimitAt75Percent

Alarm	Attributes	Applicable major release
Name: CheckpointLimitAt75Percent (425) Type: configurationAlarm Package: topology.CheckpointLimitAt75Percent Raised on class: topology.TopologyManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyCheckpoints	Release: • N/A
Description: The alarm is raised when the number of check points reaches 75 percent of the maximum allowed value.		

Table 39-119 CheckpointLimitAt75Percent (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - deprecated 9.0		

Table 39-120 CheckpointLimitReachedOrExceeded

Alarm	Attributes	Applicable major release
Name: CheckpointLimitReachedOrExceeded (426) Type: configurationAlarm Package: topology. CheckpointLimitReachedOrExceeded Raised on class: topology.TopologyManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyCheckpointObjects	Release: • N/A
Description: The alarm is raised when the number of check points objects reaches or exceeds the maximum allowed value.		
Remedial action: Maximum number of Checkpoint objects reached, the IGP history cleanup task begins and removes older objects. To keep history increase maximumNumberOfCheckpointObjects in nms-server,xml.		

Table 39-121 ChildTemplateInvalid

Alarm	Attributes	Applicable major release
Name: ChildTemplateInvalid (193) Type: configurationAlarm Package: template.ChildTemplateInvalid Raised on class: template.TemplateBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: referencedObjectInvalid	Release: • N/A
Description: The alarm is raised when a child template in a template binding is invalid. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.		
Raising condition: ('childTemplateInvalidReference' EQUAL 'true')		
Clearing condition: ('childTemplateInvalidReference' EQUAL 'false')		
Remedial action: Informational - deprecated 6.0		

Table 39-122 ChipIfCellEvent

Alarm	Attributes	Applicable major release
Name: ChipIfCellEvent (4991) Type: hardwareAnomaly Package: equipment.ChipIfCellEvent Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ifCellError	Release: • N/A
Description: The alarm is raised when an inter-chip interface (XPL2 bundle) experiences internal datapath cell errors on IOM or CPM.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-123 ChipIfDownEvent

Alarm	Attributes	Applicable major release
Name: ChipIfDownEvent (4992) Type: hardwareAnomaly Package: equipment.ChipIfDownEvent Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ifDownError	Release: • N/A
Description: The alarm is raised when an inter-chip interface (XPL2 bundle) experiences an internal datapath problem on IOM or CPM.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-124 ChipResetProtImpact

Alarm	Attributes	Applicable major release
Name: ChipResetProtImpact (5642) Type: hardwareAnomaly Package: equipment.ChipResetProtImpact Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ChipResetProtocolTimeout	Release: • N/A
Description: The alarm is raised when a slot experienced a data path failure which impacted a protocol.		
Remedial action: Informational.The alarm is raised when a slot experienced a data path failure due to Qchip reset on IOM/CPM which caused a timeout on short BFD or ETH-OAM protocol timers. Services-related data associated with the impacted protocol may be lost.		

Table 39-125 CliCommandFailure

Alarm	Attributes	Applicable major release
Name: CliCommandFailure (402) Type: communicationsAlarm Package: netw.CliCommandFailure Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cliCommandFailure	Release: • N/A
Description: The alarm is raised when a CLI command on an NE fails.		
Remedial action: Verify that the mediation profile matches the device CLI login credentials. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-126 CliConnectionProblem

Alarm	Attributes	Applicable major release
Name: CliConnectionProblem (299) Type: communicationsAlarm Package: netw.CliConnectionProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cliConnectionProblem	Release: • N/A

Table 39-126 CliConnectionProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM fails to open a CLI session on an NE because the number of open CLI sessions on the NE is at the maximum.		
Remedial action: Verify that connectivity can be established to the network element. For GNE devices, verify that the GNE profile matches the device operation.		

Table 39-127 ClientDelegateServerMaxUIExceeded

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerMaxUIExceeded (730) Type: resourceAlarm Package: server.ClientDelegateServerMaxUIExceeded Raised on class: server.ClientDelegateServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: clientDelegateServerMax-UIExceeded	Release: • N/A
Description: The alarm is raised when the total number of client GUI sessions on a client delegate server reaches or exceeds the configured maximum value.		
Remedial action: Informational - The number of available GUI client sessions has been exceeded. Please reduce the number of GUI client sessions.		

Table 39-128 CliLoginFailed

Alarm	Attributes	Applicable major release
Name: CliLoginFailed (298) Type: communicationsAlarm Package: netw.CliLoginFailed Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cliLoginFailed	Release: • N/A
Description: The alarm is raised when a CLI login attempt fails because of an incorrect user name or password.		
Remedial action: Verify that the mediation profile matches the device login credentials.		

Table 39-129 CliLoginMaxAttempts

Alarm	Attributes	Applicable major release
Name: CliLoginMaxAttempts (3701) Type: communicationsAlarm Package: netw.CliLoginMaxAttempts Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cliLoginMaxAttempts	Release: • N/A
Description: The alarm is raised when the number of CLI login failures due to an incorrect user name or password using TELNET session exceeds the configured value.		
Remedial action: The wrong password was entered by the user during telnet. Please try to log in again later.		

Table 39-130 CModeRxQueryMismatch

Alarm	Attributes	Applicable major release
Name: CModeRxQueryMismatch (160) Type: configurationAlarm Package: igmp.CModeRxQueryMismatch Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidCompatibilityMode-ofQueryReceieved	Release: • N/A
Description: The alarm is raised when an IGMP interface receives an IGMP query of a higher version than the version configured on the interface, for example, when the interface is configured for IGMPv1 and it receives an IGMPv2 or IGMPv3 query. The interface does not process the received IGMP message.		
Remedial action: Informational - no corrective action required.		

Table 39-131 ColorMismatchAlarm

Alarm	Attributes	Applicable major release
Name: ColorMismatchAlarm (8420) Type: integrityViolation Package: gmpls.ColorMismatchAlarm Raised on class: gmpls.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: colorMismatch	Release: • N/A
Description: The alarm is raised when the colors configured on the endpoints of the TE Link do not match.		
Remedial action: This alarm indicates that the colors configured on the endpoints of the discovered TE Link do not match. Please make sure the colors match.		

Table 39-132 CombinerLossOfAlignment (mwa)

Alarm	Attributes	Applicable major release
Name: CombinerLossOfAlignment (5604) Type: equipmentAlarm Package: mwa.CombinerLossOfAlignment Raised on class: mwa.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CombinerLossOfAlignment	Release: • N/A
Description: The alarm is raised when a MPT detects a combiner loss of alignment.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-133 CommunityMisconfiguration

Alarm	Attributes	Applicable major release
Name: CommunityMisconfiguration (442) Type: serviceAlarm Package: vprn.CommunityMisconfiguration Raised on class: vprn.AbstractSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CommunityMisconfiguration	Release: • N/A

Table 39-133 CommunityMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a community misconfiguration on a service site.		
Remedial action: Configure the SNMP community String on the VPRN service site		

Table 39-134 ConfigFileSyncFailed

Alarm	Attributes	Applicable major release
Name: ConfigFileSyncFailed (102) Type: equipmentAlarm Package: sw.ConfigFileSyncFailed Raised on class: sw.SoftwareUpgradeManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configFileSyncFailed	Release: • N/A
Description: The alarm is raised when the configuration file synchronization between the active and standby CPM cards fails.		
Remedial action: Please log into the NE in question via CLI and execute a manual synchronization. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-135 ConfigNotCompatible

Alarm	Attributes	Applicable major release
Name: ConfigNotCompatible (405) Type: equipmentAlarm Package: equipment.ConfigNotCompatible Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DaughterCardConfigNotCompatible	Release: • N/A
Description: The alarm is raised when an MDA configuration is incompatible with the MDA.		
Remedial action: A configuration error has occurred which must be corrected. The MDA type configured for the slot identified in the alarm must match the installed MDA type.		

Table 39-136 ContainingEquipmentMissing

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMissing (463) Type: equipmentAlarm Package: equipment.ContainingEquipmentMissing Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMissing	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMissing.		
Clearing condition: (('Status' NOT EQUAL 'Parent Removed') OR ('isTerminatable' NOT EQUAL 'true') OR ('Equipped' EQUAL 'false'))		
Remedial action: Informational - an card has been removed from the system.		

Table 39-137 CorporateAndSecuredCompositeServicesAreNotConnected

Alarm	Attributes	Applicable major release
Name: CorporateAndSecuredComposite-ServicesAreNotConnected (828) Type: serviceAlarm Package: ipsec.CorporateAndSecuredComposite-ServicesAreNotConnected Raised on class: ipsec.IPSecSecuredVpn	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CompositeServiceMisconfiguration	Release: • N/A
Description: The alarm is raised when the corporate and secured services used by an IPsec VPN do not have a connector between them.		
Raising condition: ('corporateToSecureServiceConnector' EQUAL 'Not Connected')		
Clearing condition: (('corporateToSecureServiceConnector' EQUAL 'Connected') OR ('corporateToSecureServiceConnector' EQUAL 'None'))		
Remedial action: Create a connector to connect the Corporate service and Secured service.		

Table 39-138 CorporateAndSecuredCompositeServicesMistmatch

Alarm	Attributes	Applicable major release
Name: CorporateAndSecuredComposite-ServicesMistmatch (829) Type: serviceAlarm Package: ipsec.CorporateAndSecuredCompositeServicesMistmatch Raised on class: ipsec.IPSecSecuredVpn	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CompositeServiceMisconfiguration	Release: • N/A
Description: The alarm is raised when the corporate and secured services used by an IPsec VPN are in different composite services.		
Remedial action: Informational - no corrective action required.		

Table 39-139 CorruptedBgpUpdate

Alarm	Attributes	Applicable major release
Name: CorruptedBgpUpdate (3328) Type: topologyAlarm Package: topology.CorruptedBgpUpdate Raised on class: topology.BgpAutonomousSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CorruptedBgpUpdateDetected	Release: • N/A
Description: The alarm is raised when a BGP-bad-update-packet-received message is sent from the CPAA against a BGP AS. The alarm is not auto-cleared by CPAM.		
Remedial action: A peer is sending a corrupted BGP update. The information regarding the update can be viewed in the BGP corrupted update record. Action should be taken to fix the offending BGP speaker.		

Table 39-140 CorruptedUdpPacket

Alarm	Attributes	Applicable major release
Name: CorruptedUdpPacket (1921) Type: communicationsAlarm Package: netw.CorruptedUdpPacket Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: corruptedPacket	Release: • N/A
Description: The alarm is raised when an UDP packet for an application is corrupted.		
Remedial action: A call trace packet contains unexpected content. If the problem persists, the source device might be generating unexpected content.		

Table 39-141 CostMetricMismatchAlarm

Alarm	Attributes	Applicable major release
Name: CostMetricMismatchAlarm (8421) Type: integrityViolation Package: gmpls.CostMetricMismatchAlarm Raised on class: gmpls.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: costMetricMismatch	Release: • N/A
Description: The alarm is raised when the cost metric configured on the endpoints of the TE Link do not match.		
Remedial action: This alarm indicates that the cost metric configured on the endpoints of the discovered TE Link do not match. Please make sure the cost metrics match.		

Table 39-142 CouplingEthernetLinkDown

Alarm	Attributes	Applicable major release
Name: CouplingEthernetLinkDown (4819) Type: communicationsAlarm Package: mwa.CouplingEthernetLinkDown Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfSignal	Release: • N/A
Description: The alarm is raised when a MPT detects a coupling Ethernet Link Down		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-143 CouplingLossOfRadioFrame

Alarm	Attributes	Applicable major release
Name: CouplingLossOfRadioFrame (4820) Type: communicationsAlarm Package: mwa.CouplingLossOfRadioFrame Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfFrame	Release: • N/A
Description: The alarm is raised when a MPT detects a Loss of Radio Frame from Coupling Path		

Table 39-143 CouplingLossOfRadioFrame (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-144 CouplingPortSFPCardFailure

Alarm	Attributes	Applicable major release
Name: CouplingPortSFPCardFailure (4821) Type: equipmentAlarm Package: mwa.CouplingPortSFPCardFailure Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitProblem	Release: • N/A
Description: This alarm is raised when coupling port SFP Card failure is detected.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-145 CouplingPortSFPMissing

Alarm	Attributes	Applicable major release
Name: CouplingPortSFPMissing (4822) Type: equipmentAlarm Package: mwa.CouplingPortSFPMissing Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitMissing	Release: • N/A
Description: This alarm is raised when coupling port SFP is missing.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-146 CpaaAreaUnreachableThroughISIS

Alarm	Attributes	Applicable major release
Name: CpaaAreaUnreachableThroughISIS (5418) Type: topologyAlarm Package: topology.CpaaAreaUnreachableThroughISIS Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPAALinksToAreaDown	Release: • N/A
Description: The alarm is raised when all links from CPAA to an area are down.		
Remedial action: 1) The active CPAA cannot reach certain CPAA instance through the ISIS protocol. Please check the links to the unreachable CPAA instance.\n2) If the standby CPAA is functional as per your requirements, switch-over might resolve the issue.		

Table 39-147 CpaaAreaUnreachableThroughOSPF

Alarm	Attributes	Applicable major release
Name: CpaaAreaUnreachableThroughOSPF (5419) Type: topologyAlarm Package: topology. CpaaAreaUnreachableThroughOSPF Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPAALinksToAreaDown	Release: • N/A
Description: The alarm is raised when all links from CPAA to OSPF area are down.		
Remedial action: 1) The active CPAA cannot reach certain area through the OSPF protocol. Please check the links to the unreachable area.\n2) If the standby CPAA is functional as per your requirements, switch-over might resolve the issue.		

Table 39-148 CpaaAreaUnreachableThroughOSPFv3

Alarm	Attributes	Applicable major release
Name: CpaaAreaUnreachableThroughOSPFv3 (5420) Type: topologyAlarm Package: topology. CpaaAreaUnreachableThroughOSPFv3 Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CPAALinksToAreaDown	Release: • N/A
Description: The alarm is raised when all links from CPAA to OSPFv3 area are down.		
Remedial action: 1) The active CPAA cannot reach certain area through the OSPFv3 protocol. Please check the links to the unreachable area.\n2) If the standby CPAA is functional as per your requirements, switch-over might resolve the issue.		

Table 39-149 CpamTimedLicenseExpiryNotice

Alarm	Attributes	Applicable major release
Name: CpamTimedLicenseExpiryNotice (692) Type: cpamLicensingAlarm Package: security.CpamTimedLicenseExpiryNotice Raised on class: security.CpamLicense	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: timedcpamLicenseExpiryNotice	Release: • N/A
Description: The alarm is raised when the 5650 CPAM license timer expires. The alarm information includes the license expiry date.		
Remedial action: Informational - the CPAM license key is about to expire. Please contact your Nokia sales representative to request either an extension for the license or a permanent license key.		

Table 39-150 CpeUnreachable

Alarm	Attributes	Applicable major release
Name: CpeUnreachable (525) Type: communicationsAlarm Package: rtr.CpeUnreachable Raised on class: rtr.StaticRoute	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CpeUnreachable	Release: • N/A
Description: The alarm is raised when the CPE associated with a static route is unreachable.		
Remedial action: Please check that the static route is correct or exists for the CPE.		

Table 39-151 CPMPChipMemoryEvent

Alarm	Attributes	Applicable major release
Name: CPMPChipMemoryEvent (4989) Type: hardwareAnomaly Package: equipment.CPMPChipMemoryEvent Raised on class: equipment.ProcessorCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: memoryParityError	Release: • N/A
Description: The alarm is raised when a PChip detects a memory error. The alarm is raised against a 7450 ESS, 7710 SR, 7950 SR, or 7750 SR. The alarm is raised against a Release 11.0 NE at R4 or later.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-152 CreditControlInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: CreditControlInsertedFltrEntryDropped (1150) Type: configurationAlarm Package: aclfilter. CreditControlInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • N/A
Description: The alarm is raised when a request to insert a filter entry is not successful for a credit control application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for Credit Control application. Check the configuration filter entry.		

Table 39-153 CreditControlInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: CreditControlInsertSpaceThresholdAlarm (1149) Type: configurationAlarm Package: aclfilter. CreditControlInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • N/A
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a credit control application insert range.		
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for Credit Control application. Make an adjusted to the high watermark or to the filter.		

Table 39-154 CRLAfterExpWarning

Alarm	Attributes	Applicable major release
Name: CRLAfterExpWarning (9597) Type: communicationsAlarm Package: sitesec.CRLAfterExpWarning Raised on class: sitesec.CertificateAuthProfile	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CRLAfterExpWarning	Release: • N/A
Description: The alarm is raised when the CRL file indicated in Certificate Authority profile is expired.		
Remedial action: Replace the indicated file with an updated CRL.		

Table 39-155 CRLBeforeExpWarning

Alarm	Attributes	Applicable major release
Name: CRLBeforeExpWarning (9598) Type: communicationsAlarm Package: sitesec.CRLBeforeExpWarning Raised on class: sitesec.CertificateAuthProfile	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: CRLBeforeExpWarning	Release: • N/A
Description: The alarm is raised when the CRL file indicated in Certificate Authority profile will expire in the time period as indicated.		
Remedial action: Replace the indicated file with an updated CRL.		

Table 39-156 CRLUpdateFailureonAllURL

Alarm	Attributes	Applicable major release
Name: CRLUpdateFailureonAllURL (9599) Type: communicationsAlarm Package: sitesec.CRLUpdateFailureonAllURL Raised on class: sitesec.CrlUrlEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crlUpdateFailureonAllURL	Release: • N/A

Table 39-156 CRLUpdateFailureonAllURL (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the CRL update operation failed after attempting all URLs for an existing CA Profile.		
Remedial action: Make sure the URLs specified in CrlUrlEntry is correct.		

Table 39-157 CRLUpdateFailureonURL

Alarm	Attributes	Applicable major release
Name: CRLUpdateFailureonURL (9600) Type: communicationsAlarm Package: sitesec.CRLUpdateFailureonURL Raised on class: sitesec.CrlUrlEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: crlUpdateFailureonURL	Release: • N/A
Description: The alarm is raised when the CRL update operation has failed after attempting the indicated URL for an existing CA Profile.		
Remedial action: Make sure the URLs specified in CrlUrlEntry is correct.		

Table 39-158 CurrentDataMergeTableCountThresholdExceeded

Alarm	Attributes	Applicable major release
Name: CurrentDataMergeTableCount-ThresholdExceeded (9616) Type: databaseAlarm Package: db.CurrentDataMergeTableCountThresholdExceeded Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: This alarm indicated that the auxiliary database is unable to keep up with the update rate for current data during stats collection. The number of pending merges is above the threshold. It is a sign that stats collection is falling behind. Your auxiliary database cluster capacity might not be capable of handling the stats collection load.		
Remedial action: Try increasing the threshold for merge tables. If this does not work. Please revisit the capacity of the auxiliary database cluster.		

Table 39-159 CurrentDataMergeTableCountTooHigh

Alarm	Attributes	Applicable major release
Name: CurrentDataMergeTableCountTooHigh (9617) Type: databaseAlarm Package: db.CurrentDataMergeTableCountTooHigh Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A

Table 39-159 CurrentDataMergeTableCountTooHigh (continued)

Alarm	Attributes	Applicable major release
Description: This alarm indicated that the auxiliary database is unable to keep up with the update rate for current data during stats collection. The number of pending merges is above expected with respect to the number of routers/stats types being collected. It is a sign that stats collection is falling behind. Your auxiliary database cluster capacity might not be capable of handling the stats collection load.		
Remedial action: Decrease the number of performance stats being collected or decrease the number of routers subject to mib statistics collection or increase the capacity of the auxiliary database cluster.		

Table 39-160 CurrentDataMergeTableTooOld

Alarm	Attributes	Applicable major release
Name: CurrentDataMergeTableTooOld (9618) Type: databaseAlarm Package: db.CurrentDataMergeTableTooOld Raised on class: db.AuxiliaryDatabaseCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: This alarm indicated that the auxiliary database is unable to keep up with the update rate for current data during stats collection. Some merge tables stayed in the system longer than the allowed time threshold. It is a sign that stats collection is falling behind. Your auxiliary database cluster capacity might not be capable of handling the stats collection load.		
Remedial action: Revisit the capacity of the auxiliary database cluster with respect to the amount of performance stats collected.		

Table 39-161 DatabaseArchivedLogNotApplied

Alarm	Attributes	Applicable major release
Name: DatabaseArchivedLogNotApplied (205) Type: configurationAlarm Package: db.DatabaseArchivedLogNotApplied Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: databaseArchivedLogNotApplied	Release: • N/A
Description: The alarm is raised when, during a database backup, the 5620 SAM determines that the archive logs are not being applied to the standby database, as indicated by the archive log gap. The archive log gap threshold is defined in the nms-server.xml file. The alarm is raised only in a redundant 5620 SAM system.		
Remedial action: Possible causes include loss of network connectivity between the primary and standby database platforms or network latency. If problem does not appear to be network connectivity/latency related then please contact your Nokia support representative for assistance.		

Table 39-162 DatabaseBackupFailed

Alarm	Attributes	Applicable major release
Name: DatabaseBackupFailed (136) Type: configurationAlarm Package: db.DatabaseBackupFailed Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: databaseBackupFailure	Release: • N/A
Description: The alarm is raised when the database backup files cannot be created because of, for example, a lack of disk space or insufficient file permissions.		
Remedial action: Check the additional text of the alarm for guidance as to the specifics of the problem. Possible causes are lack of disk space or insufficient file permissions or the backup cannot finish on time. If the backup cannot finish on time, re-attempt the database backup.		

Table 39-163 DatabaseBackupInvalidConfig

Alarm	Attributes	Applicable major release
Name: DatabaseBackupInvalidConfig (1117) Type: configurationAlarm Package: db.DatabaseBackupInvalidConfig Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InvalidbBackupConfigration	Release: • N/A
Description: The alarm is raised when the directory location specified for database scheduled backups is empty.		
Remedial action: A configuration error has been made which must be corrected. The backup destination must be configured in the database backup policy.		

Table 39-164 DatabaseBackupRsyncFailed

Alarm	Attributes	Applicable major release
Name: DatabaseBackupRsyncFailed (749) Type: databaseAlarm Package: db.DatabaseBackupRsyncFailed Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: databaseBackupFileRsync-Failed	Release: • N/A
Description: The alarm is raised when one or more database backup files cannot be copied to the standby database station.		
Remedial action: The additional text field of the alarm will provide more details as will the EmsServer.log. Possible causes include a HW failure on the platform hosting the standby database function, loss of network connectivity between the primary and standby database servers.		

Table 39-165 DatabaseRedundancyArchiveGap

Alarm	Attributes	Applicable major release
Name: DatabaseRedundancyArchiveGap (611) Type: configurationAlarm Package: db.DatabaseRedundancyArchiveGap Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DatabaseRedundancyArchive-Gap	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM main server detects an archive log gap. An archive log gap occurs when a number of archive logs cannot be applied to the standby database. The alarm may indicate that the primary database is out of archive log disk space, the standby database has been down for too long, or the standby database is not able to process the archive logs at the rate that the primary database sends them. The alarm clears after a standby database reinstantiation, which corrects the archive log gap. The alarm is raised only in a redundant 5620 SAM system.		
Remedial action: The standby database should be manually re-instantiated using the commands available in the SAM GUI. Please contact your Nokia support representative for further investigation.		

Table 39-166 DatabaseRedundancyFailure

Alarm	Attributes	Applicable major release
Name: DatabaseRedundancyFailure (246) Type: configurationAlarm Package: db.DatabaseRedundancyFailure Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DatabaseRedundancyFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a standby database problem, for example, the database is down or not in managed recovery mode. The alarm clears when the standby database is functional. The alarm is raised only in a redundant 5620 SAM system.		
Remedial action: The additional text field of the alarm will provide more details as will the EmsServer.log. Possible causes include a HW failure on the platform hosting the standby database function, loss of network connectivity between the primary and standby database		

Table 39-167 DatabaseRedundancyOutOfSync

Alarm	Attributes	Applicable major release
Name: DatabaseRedundancyOutOfSync (302) Type: configurationAlarm Package: db.DatabaseRedundancyOutOfSync Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DatabaseRedundancyOutOf-Sync	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM server polls the primary and standby databases and detects a difference in the primary and standby database archive log sequence numbers that is greater than one. The alarm may indicate that the primary database is not sending archive logs to the standby quickly enough, or that the standby database is not able to process the archive logs at the rate that the primary sends them. The alarm is raised only in a redundant 5620 SAM system.		

Table 39-167 DatabaseRedundancyOutOfSync (continued)

Alarm	Attributes	Applicable major release
Remedial action: Possible causes include loss of network connectivity between the primary and standby database platforms or network latency. Ensure that network connectivity is available and that network latency is within limits published by Nokia. If the network is functioning contact your Nokia support representative for assistance.		

Table 39-168 DatabaseRedundancyRealTimeApplyFailure

Alarm	Attributes	Applicable major release
Name: DatabaseRedundancyRealTimeApplyFailure (296) Type: configurationAlarm Package: db.DatabaseRedundancyRealTimeApplyFailure Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DatabaseRedundancyReal-TimeApplyFailure	Release: • N/A
Description: The alarm is raised when database redundancy falls out of real-time apply transfer mode, which means that the primary database transactions are not immediately replicated to the standby database. The alarm clears when the database is operating in real-time apply mode.		
Remedial action: Possible causes include loss of network connectivity between the primary and standby database platforms or network latency. This can be intermittent where the software will recover from this state. Ensure that network connectivity is available and that network latency is within limits published by Nokia. If the network is functioning contact your Nokia support representative for assistance.		

Table 39-169 DatabaseServerErrors

Alarm	Attributes	Applicable major release
Name: DatabaseServerErrors (5174) Type: databaseAlarm Package: db.DatabaseServerErrors Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DatabaseErrors	Release: • N/A
Description: The alarm is raised when when a critical Oracle error occurs.		
Remedial action: The probable cause of this alarm is the database server detected a critical error. The EmsDbServerHealth.log and oracle trace files will provide more information.		

Table 39-170 DatabaseSqlFormatInvalid

Alarm	Attributes	Applicable major release
Name: DatabaseSqlFormatInvalid (4419) Type: databaseAlarm Package: db.DatabaseSqlFormatInvalid Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidSqlFormat	Release: • N/A

Table 39-170 DatabaseSqlFormatInvalid (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an invalid SQL is detected by the database server.		
Remedial action: The probable cause of this alarm is the database server detected invalid SQL. The EmsDbServerHealth.log will provide more information. Possible causes include SQL injection and invalid SQL statement errors.		

Table 39-171 DataBearerPropertyMismatch

Alarm	Attributes	Applicable major release
Name: DataBearerPropertyMismatch (8391) Type: operationalViolation Package: lmp.DataBearerPropertyMismatch Raised on class: lmp.DataBearer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteIdMismatch	Release: • N/A
Description: The alarm is raised when a Data Bearer property mismatch is detected on the node. This notification is only generated the first time a mismatch is detected.		
Remedial action: A network configuration issue has been detected. Ensure the Data Bearer configuration between the local node and the peer node is consistent.		

Table 39-172 DataChannelLoopback

Alarm	Attributes	Applicable major release
Name: DataChannelLoopback (3945) Type: configurationAlarm Package: tdmequipment.DataChannelLoopback Raised on class: tdmequipment.DataChannelSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dataChannelLoopback	Release: • N/A
Description: The alarm is raised when an NE reports that a data channel has a loopback alarm condition.		
Remedial action: Informational only.		

Table 39-173 DataFileDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: DataFileDiskSpaceBelowThreshold (196) Type: databaseAlarm Package: db.DataFileDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary or standalone database data file disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: Informational - it may be necessary to add additional disk capacity to the platform. Please contact your Nokia support representative for assistance.		

Table 39-174 DatafileSizeAboveThreshold

Alarm	Attributes	Applicable major release
Name: DatafileSizeAboveThreshold (750) Type: databaseAlarm Package: db.DatafileSizeAboveThreshold Raised on class: db.DatabaseManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighNumberOfRecords	Release: • N/A
Description: The alarm is raised when a tablespace data file size exceeds the used space threshold.		
Remedial action: The probable cause of this alarm is the storage of too many records in the database. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-175 DataLossAlarm (equipment)

Alarm	Attributes	Applicable major release
Name: DataLossAlarm (148) Type: storageAlarm Package: equipment.DataLossAlarm Raised on class: equipment.FlashMemory	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dataLoss	Release: • N/A
Description: The alarm is raised when a device detects an error while writing to a compact flash unit.		
Remedial action: The frequency at which accounting statistics are being collected must be reduced. Optionally an statistics AUX server may be added to the SAM platform complex in order to offload the statistics collection task from the main SAM server.		

Table 39-176 DataLossAlarm (sw)

Alarm	Attributes	Applicable major release
Name: DataLossAlarm (148) Type: storageAlarm Package: sw.DataLossAlarm Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dataLoss	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives the tmnxLogAccountingDataLoss trap, which is sent when a statistics collection interval ends while an NE is writing data to an accounting file. The statistics collection for the interval stops immediately, and collection for the next interval begins. The accounting statistics file for the interrupted collection contains an incomplete data set as a result.		
Remedial action: The collection interval configured on the NE is too short. Please lengthen the collection interval such that the NE has sufficient time to complete data collection within one interval. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-177 DataMtReused

Alarm	Attributes	Applicable major release
Name: DataMtReused (361) Type: dataMtReusedAlarm Package: pim.DataMtReused Raised on class: pim.DataMtInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DataMtReused	Release: • N/A
Description: The alarm is raised when a data MDT is reused.		
Remedial action: A configuration error has occurred that must be corrected. Please check MVPN Selective Tunnel Data MT Interface configuration so that no duplicate C (S,G) is mapped to a data MDT.		

Table 39-178 DaughterCardConfigNotCompatible

Alarm	Attributes	Applicable major release
Name: DaughterCardConfigNotCompatible (404) Type: equipmentAlarm Package: equipment. DaughterCardConfigNotCompatible Raised on class: equipment.DaughterCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DaughterCardConfigNotCompatible	Release: • N/A
Description: The alarm is raised when a supported MDA is inserted into a compatible IOM slot, but the configuration on the MDA ports is not compatible with the MDA.		
Remedial action: A configuration error has occurred which must be corrected. The configuration of one or more ports must be changed to match the ports on the MDA.		

Table 39-179 DBFailOver

Alarm	Attributes	Applicable major release
Name: DBFailOver (201) Type: configurationAlarm Package: db.DBFailOver Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: databasePrimaryDown	Release: • N/A
Description: The alarm is raised when a database failover occurs. A standby database reinstantiation is required. The alarm clears when the standby database is online.		
Remedial action: The standby database should be manually re-instantiated using the commands available in the SAM GUI.		

Table 39-180 DDosCardFpEventOverflow

Alarm	Attributes	Applicable major release
Name: DDosCardFpEventOverflow (4460) Type: securityServiceOrMechanismViolation Package: equipment.DDosCardFpEventOverflow Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: eventOverflow	Release: • N/A
Description: The alarm is raised when a flood of distributed CPU FP protection events occur on a particular card and some of the events are lost due to event throttling mechanism.		
Remedial action: Please reduce the number of distributed DoS FP protection policers configured.		

Table 39-181 DDosCardSapEventOverflow

Alarm	Attributes	Applicable major release
Name: DDosCardSapEventOverflow (4461) Type: securityServiceOrMechanismViolation Package: equipment.DDosCardSapEventOverflow Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: eventOverflow	Release: • N/A
Description: The alarm is raised when a flood of distributed CPU protection SAP events occur on a particular card and some of the events are lost due to event throttling mechanism.		
Remedial action: Please reduce the number of distributed DoS SAP protection policers configured.		

Table 39-182 DDosCardVrtrIfEventOverflow

Alarm	Attributes	Applicable major release
Name: DDosCardVrtrIfEventOverflow (4462) Type: securityServiceOrMechanismViolation Package: equipment.DDosCardVrtrIfEventOverflow Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: eventOverflow	Release: • N/A
Description: The alarm is raised when a flood of distributed CPU protection network-interface events occur on a particular card and some of the events are lost due to event throttling mechanism.		
Remedial action: Please reduce the number of distributed DoS Network Interface protection policers configured.		

Table 39-183 DDosFpDynamicPoolUsageHigh

Alarm	Attributes	Applicable major release
Name: DDosFpDynamicPoolUsageHigh (4463) Type: securityServiceOrMechanismViolation Package: equipment.DDosFpDynamicPoolUsageHigh Raised on class: equipment.ForwardingPlane	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A

Table 39-183 DDosFpDynamicPoolUsageHigh (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the dynamic enforcement policer pool usage on the forwarding plane is nearly exhausted.		
Remedial action: Please adjust the dynamic enforcement policer pool usage.		

Table 39-184 DefaultInstanceInconsistency

Alarm	Attributes	Applicable major release
Name: DefaultInstanceInconsistency (211) Type: ConfigurationAlarm Package: policy.DefaultInstanceInconsistency Raised on class: policy.Manager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: multipleDefaultInstancesEncountered	Release: • N/A
Description: The alarm is raised when an accounting policy is the default for more then one service type or more then one network type.		
Raising condition: ('defaultInstanceInconsistency' EQUAL 'true')		
Clearing condition: ('defaultInstanceInconsistency' EQUAL 'false')		
Remedial action: Informational		

Table 39-185 Degrade

Alarm	Attributes	Applicable major release
Name: Degrade (622) Type: communicationsAlarm Package: equipment.Degrade Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: degrade	Release: • N/A
Description: The alarm is raised when a degraded signal is detected.		
Remedial action: The signal being received on the indicated port is of poor quality. Check to ensure that the physical link is not damaged and that the link is properly connected/seated to the port.		

Table 39-186 DemodulatorUnlocked

Alarm	Attributes	Applicable major release
Name: DemodulatorUnlocked (4823) Type: communicationsAlarm Package: mwa.DemodulatorUnlocked Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DemodulationFailure	Release: • N/A
Description: The alarm is raised when a MPT detects demodulation failure.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-187 DependentObjectDeleted

Alarm	Attributes	Applicable major release
Name: DependentObjectDeleted (192) Type: configurationAlarm Package: template.DependentObjectDeleted Raised on class: template.Template	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: referencedObjectGone	Release: • N/A
Description: The alarm is raised when an object referenced by a template cannot be found. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.		
Raising condition: ('Invalid References (Reset on Save)' EQUAL 'true')		
Clearing condition: ('Invalid References (Reset on Save)' EQUAL 'false')		
Remedial action: Informational - deprecated 6.0		

Table 39-188 DeployerObjectsLimitExceeded

Alarm	Attributes	Applicable major release
Name: DeployerObjectsLimitExceeded (3314) Type: communicationsAlarm Package: netw.DeployerObjectsLimitExceeded Raised on class: netw.NmsSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyDeployerObjects	Release: • N/A
Description: The alarm is raised when the number of deployed objects or attributes exceeds the 5620 SAM system limit.		
Remedial action: Clear failed deployers to make deployers available for network operations.		

Table 39-189 DeploymentFailure

Alarm	Attributes	Applicable major release
Name: DeploymentFailure (13) Type: deploymentFailure Package: generic.DeploymentFailure Raised on class: generic.GenericObject	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedToModifyNetworkResource	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to create, modify, or delete a network object because of NE unreachability or a failed SNMP set operation. The alarm information includes the deployment ID, the requesting user ID, and the deployment type.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM		

Table 39-190 DeployProfileFailed

Alarm	Attributes	Applicable major release
Name: DeployProfileFailed (610) Type: configurationAlarm Package: autoconfig.DeployProfileFailed Raised on class: autoconfig.AutoProvisioning	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DeployProfileFailed	Release: • N/A
Description: The alarm is raised when the deployment of a script to a 7705 SAR fails.		
Remedial action: Informational - Please revisit target node configuration.		

Table 39-191 DetectedPreProvisionedCantidateNodeHasConfig

Alarm	Attributes	Applicable major release
Name: DetectedPreProvisionedCanti-dateNodeHasConfig (1960) Type: communicationsAlarm Package: netw. DetectedPreProvisionedCantidateNodeHasConfig Raised on class: netw.DiscoveredNode	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: detectedPreProvisionedCanti-dateNodeHasConfig	Release: • N/A
Description: The alarm is raised when the candidate node detected for pre-provisioning already has a configuration in it. The configuration in the detected node is replaced with the configuration in the matching pre-provisioned node in SAM during the deployment stage of self-configuration.		
Remedial action: Verify that the candidate network element is intended to be pre-provisioned with the specified configuration. configuration deployment stage of self-config		

Table 39-192 DfPeerDown

Alarm	Attributes	Applicable major release
Name: DfPeerDown (3304) Type: EpcLIAlarm Package: lteli.DfPeerDown Raised on class: lteli.DFPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DfPeerDown	Release: • N/A
Description: The alarm is raised on a Delivery Function that is operationally down.		
Raising condition: (('isLocal' EQUAL 'true') AND ('Operational State' NOT EQUAL 'In Service'))		
Clearing condition: NOT ((('isLocal' EQUAL 'true') AND ('Operational State' NOT EQUAL 'In Service')))		
Remedial action: A TCP connection failure associated with a Delivery Function has occurred. The underlying transport network is unreliable. Please correct the issue within the transport network.		

Table 39-193 DHCPPFoLeaseUpdateFailedAddressConflict

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedAddressConflict (5159) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedAddressConflict Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedAddressConflict	Release: • N/A
Description: This alarm is raised when a address conflict lease update received from the failover peer cannot be processed successfully. This DHCP pool instance has already leased another address to this host.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. This DHCP pool instance has already leased another address to this host. Please ensure all configurations are correct.		

Table 39-194 DHCPPFoLeaseUpdateFailedfoShutdown

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedfoShutdown (5167) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedfoShutdown Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedfoShutdown	Release: • N/A
Description: This alarm is raised when a shutdown lease update received from the failover peer cannot be processed successfully. The failover state of this DHCP Pool instance is 'shutdown'.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. The failover state of this DHCP Pool instance is 'shutdown'. Please ensure all configurations are correct.		

Table 39-195 DHCPPFoLeaseUpdateFailedHostConflict

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedHostConflict (5160) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedHostConflict Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedHostConflict	Release: • N/A
Description: This alarm is raised when a host conflict lease update received from the failover peer cannot be processed successfully. This DHCP pool instance has already leased this address to another host.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. This DHCP pool instance has already leased this address to another host. Please ensure all configurations are correct.		

Table 39-196 DHCPPFoLeaseUpdateFailedLeaseExpired

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedLeaseExpired (5161) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedLeaseExpired Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedLeaseExpired	Release: • N/A
Description: This alarm is raised when a lease expired lease update received from the failover peer cannot be processed successfully. The lease received from the peer has expired.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. The lease received from the peer has expired. Please ensure all configurations are correct.		

Table 39-197 DHCPPFoLeaseUpdateFailedMaxLeaseReached

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedMax-LeaseReached (5162) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedMaxLeaseReached Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedMaxLeaseReached	Release: • N/A
Description: This alarm is raised when a maximum reached lease update received from the failover peer cannot be processed successfully. The maximum number of leases is already reached.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. The maximum number of leases is already reached. Please ensure all configurations are correct.		

Table 39-198 DHCPPFoLeaseUpdateFailedPeerConflict

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedPeerConflict (5163) Type: configurationAlarm Package: dhcp. DHCPPFoLeaseUpdateFailedPeerConflict Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdate-FailedPeerConflict	Release: • N/A
Description: This alarm is raised when a peer conflict lease update received from the failover peer cannot be processed successfully. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP pool instance.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. The failover peer has leased an address within a subnet range of which the failover control is set to 'local' on this local DHCP pool instance. Please ensure all configuration is correct.		

Table 39-199 DHCPPFoLeaseUpdateFailedPersistenceCongested

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedPersistenceCongested (5164) Type: configurationAlarm Package: dhcp.DHCPPFoLeaseUpdateFailedPersistenceCongested Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdateFailedPersistenceCongested	Release: • N/A
Description: This alarm is raised when a persistence congested lease update received from the failover peer cannot be processed successfully. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. The lease received from the peer can not be persistently stored because the persistence subsystem is in overload. Please ensure all configuration is correct.		

Table 39-200 DHCPPFoLeaseUpdateFailedRangeNotFound

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedRangeNotFound (5165) Type: configurationAlarm Package: dhcp.DHCPPFoLeaseUpdateFailedRangeNotFound Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdateFailedRangeNotFound	Release: • N/A
Description: This alarm is raised when a range not found lease update received from the failover peer cannot be processed successfully. No valid include range for this lease could be found.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. No valid include range for this lease could be found. Please ensure all configurations are correct.		

Table 39-201 DHCPPFoLeaseUpdateFailedSubnetNotFound

Alarm	Attributes	Applicable major release
Name: DHCPPFoLeaseUpdateFailedSubnetNotFound (5166) Type: configurationAlarm Package: dhcp.DHCPPFoLeaseUpdateFailedSubnetNotFound Raised on class: dhcp.LocalDhcpPoolFailover	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DHCPPFoLeaseUpdateFailedSubnetNotFound	Release: • N/A
Description: This alarm is raised when a subnet not found lease update received from the failover peer cannot be processed successfully. No valid subnet for this lease could be found.		
Remedial action: This alarm indicates that the Local DHCP Pool Failover lease update has failed. Packets received from the failover peer cannot be processed. No valid subnet for this lease could be found. Please ensure all configurations are correct.		

Table 39-202 DhcpServerAddrAllocationFailure

Alarm	Attributes	Applicable major release
Name: DhcpServerAddrAllocationFailure (11064) Type: configurationAlarm Package: dhcp.DhcpServerAddrAllocationFailure Raised on class: dhcp.LocalDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpsAddrAllocationFailure	Release: • N/A
Description: This alarm is raised when a DHCP server instance could not allocate an address for a client. [CAUSE] A failure occurs when a DHCP server instance could not allocate an address for a client. The reason could be that the DHCP server instance could not find a free address, or it could be a configuration issue. [EFFECT] The client does not get an IP address lease this time. The client will have to try again if it needs a lease from this system. [RECOVERY] The recovery action, if any, will depend on the reason.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-203 DhcpServerHostConflict

Alarm	Attributes	Applicable major release
Name: DhcpServerHostConflict (11065) Type: configurationAlarm Package: dhcp.DhcpServerHostConflict Raised on class: dhcp.LocalDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrHostConflict	Release: • N/A
Description: This alarm is raised when when a host requests an fixed IP address in the local user database and the system detects that this IP address has alread been handed out to another (dynamic) host. [RECOVERY] The recovery action, if any, will depend on the reason.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-204 DhcpServerIntLseConflict

Alarm	Attributes	Applicable major release
Name: DhcpServerIntLseConflict (11066) Type: configurationAlarm Package: dhcp.DhcpServerIntLseConflict Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrIntLseConflict	Release: • N/A
Description: This alarm is raised when DHCP hosts trying to acquire an IP address that was handed through the local address assignment infrastructure, or the local address assignment infrastructure tries to use an IP address that was handed out to a DHCP client. [RECOVERY] The recovery action, if any, will depend on the reason.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-205 DhcpServerLeaseNotOwner

Alarm	Attributes	Applicable major release
Name: DhcpServerLeaseNotOwner (11067) Type: configurationAlarm Package: dhcp.DhcpServerLeaseNotOwner Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrLeaseNotOwner	Release: • N/A
Description: This alarm is raised when a DHCP message is received from a DHCP client that does not own the lease indicated by the IP address from the message. [RECOVERY] The recovery action, if any, will depend on the reason.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-206 DhcpServerLeaseOfferedExpired

Alarm	Attributes	Applicable major release
Name: DhcpServerLeaseOfferedExpired (11068) Type: configurationAlarm Package: dhcp.DhcpServerLeaseOfferedExpired Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpsLeaseOfferedExpired	Release: • N/A
Description: This alarm is raised when an offered DHCP lease expires in the 'offered' state. [CAUSE] A failure occurs when a DHCP lease that this system had offered to a client, expires while it is still in the 'offered' state, because this system did not receive a DHCP request message from the client. [EFFECT] The client does not get a lease this time. The client will have to try again if it needs a lease from this system. [RECOVERY] The recovery action, if any, will depend on the reason of the expiry.		
Remedial action: The recovery action, if any, will depend on the reason of the expiry.		

Table 39-207 DhcpServerPoolUnknown

Alarm	Attributes	Applicable major release
Name: DhcpServerPoolUnknown (11069) Type: configurationAlarm Package: dhcp.DhcpServerPoolUnknown Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpSvrPoolUnknown	Release: • N/A
Description: This alarm is raised when when the lookup in the local user database for a host returns a poolname which is not defined within the local DHCP server. [RECOVERY] The recovery action, if any, will depend on the reason.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-208 DiamMessageDropped

Alarm	Attributes	Applicable major release
Name: DiamMessageDropped (9639) Type: processingErrorAlarm Package: diameter.DiamMessageDropped Raised on class: diameter.DiameterPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diamMessageDropped	Release: • N/A
Description: The alarm is raised when the Diameter protocol has dropped a message.		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Info form for a specific cause for the failure.		

Table 39-209 DiamSessionEventFailure

Alarm	Attributes	Applicable major release
Name: DiamSessionEventFailure (8379) Type: processingErrorAlarm Package: diameter.DiamSessionEventFailure Raised on class: diameter.DiameterAppPolicy	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownApplicationPolicy Applicable probable causes: • UnknownApplicationPolicy • UnknownPeerPolicy • NoOperationalPeers • TxError • RxError • TxTimeout • TxTimeoutPendingQ • TxRetriesExceeded • CcrtReplayLifetimeExceeded • CcrtReplayTooManySessions	Release: • N/A
Description: This alarm is raised when something unusual happens while handling a Diameter session.		
Remedial action: The recovery action depends on the exact cause of the failure. See the Additional Text field in the Alarm Information form for a specific cause for the failure.		

Table 39-210 DiskCapacityProblem

Alarm	Attributes	Applicable major release
Name: DiskCapacityProblem (144) Type: storageAlarm Package: equipment.DiskCapacityProblem Raised on class: equipment.FlashMemory	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskCapacityProblem	Release: • N/A

Table 39-210 DiskCapacityProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a compact flash capacity threshold value on an NE is reached or exceeded. The alarm condition is detected during resynchronization or when a tnmxEqFlashDiskFull trap is received. The threshold value is not configurable. The severity of the alarm depends on the percentage of disk capacity used, as listed below: - 75 percent, Minor - 90 percent, Major - 100 percent, Critical		
Remedial action: The usage of the compact flash device must be analysed and old or redundant files must be removed. This operation must be executed using the CLI interface on the NE.		

Table 39-211 DiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: DiskSpaceBelowThreshold (1934) Type: serverAlarm Package: server.DiskSpaceBelowThreshold Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the disk space threshold is reached.		
Remedial action: This is a generic error if SAM Server free disk space is below acceptable levels. The additional text field of the alarm will provide more details of the specific problem. Reduce the disk space by changing file retention times or disk usage limits. It may be necessary to add additional disk space to the system to resolve the problem.		

Table 39-212 DnsIpCacheFull

Alarm	Attributes	Applicable major release
Name: DnsIpCacheFull (8388) Type: equipmentAlarm Package: isa.DnsIpCacheFull Raised on class: isa.AaGroupMember	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DnsIpCacheFull	Release: • N/A
Description: The alarm is raised when the number of entries in a DNS IP Cache is greater than or equal to the percentage value tmnxBsxDnsIpCacheHighWatermark of its tmnxBsxDnsIpCacheSize and the previous percentage value was less than this threshold. And it is clear when the number of entries in a DNS IP Cache is less than or equal to the percentage value tmnxBsxDnsIpCacheLow-Watermark of its tmnxBsxDnsIpCacheSize and the previous percentage value was greater than this threshold.		
Remedial action: The ISA-AA DNS IP Cache buffer has entered an overload state as determined by the configured DNS IP Cache Watermarks and Size. The Watermark thresholds and or Size configured should be revisited to ensure the high threshold is not set too low, and the low threshold is not set too high with respect to the size. To disable the notification, set the High Watermark and or size to the maximum, or set the Low Watermark to the minimum.		

Table 39-213 DroppedUdpPackets

Alarm	Attributes	Applicable major release
Name: DroppedUdpPackets (1935) Type: communicationsAlarm Package: server.DroppedUdpPackets Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyUdpPacketsBuffered	Release: • N/A
Description: The alarm is raised when the number of UDP Packets that await processing by the 5620 SAM surpasses the server's capacity to process them.		
Remedial action: The NEs in the network are sending more data to this server than it can process. Reduce the number of nodes sending data to this server.		

Table 39-214 DryContactAlarm

Alarm	Attributes	Applicable major release
Name: DryContactAlarm (460) Type: dryContactAlarm Package: equipment.DryContactAlarm Raised on class: equipment.DryContact	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dryContactExternalAlarm-Raised	Release: • N/A
Description: The alarm is raised when a device detects a dry contact alarm condition.		
Remedial action: The remedial action for this alarm depends on the condition that the dry contact alarm is configured.		

Table 39-215 DS1E1Loopback

Alarm	Attributes	Applicable major release
Name: DS1E1Loopback (409) Type: configurationAlarm Package: tdmequipment.DS1E1Loopback Raised on class: tdmequipment. DS1E1ChannelSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ds1e1Loopback	Release: • N/A
Description: The alarm is raised when an NE reports that a specific DS1 or E1 channel has a loopback alarm condition.		
Remedial action: Informational only.		

Table 39-216 DS3E3Loopback

Alarm	Attributes	Applicable major release
Name: DS3E3Loopback (408) Type: configurationAlarm Package: tdmequipment.DS3E3Loopback Raised on class: tdmequipment.DS3E3ChannelSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ds3e3Loopback	Release: • N/A
Description: The alarm is raised when an NE reports that a specific DS3 or E3 channel has a loopback alarm condition.		
Remedial action: Informational only.		

Table 39-217 DualEndedLossNotSupported

Alarm	Attributes	Applicable major release
Name: DualEndedLossNotSupported (1194) Type: oamAlarm Package: ethernetoam.DualEndedLossNotSupported Raised on class: ethernetoam.MaintAssociation	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dualEndedLossNotSupported	Release: • N/A
Description: The alarm is raised when a MEP that does not support Y1731 Dual Ended Loss test is participating in a CFM Continuity Check test that has Y1731 Dual Ended Loss test enabled.		
Remedial action: Informational - The alarm is raised when at least one MEP that does not support Y1731 Dual Ended Loss test is participating in a CFM Continuity Check test that has Y1731 Dual Ended Loss test enabled.		

Table 39-218 DualEndedLossThresholdAlarm

Alarm	Attributes	Applicable major release
Name: DualEndedLossThresholdAlarm (1195) Type: oamAlarm Package: ethernetoam.DualEndedLossThresholdAlarm Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: dualEndedLossThresholdExceeded	Release: • N/A
Description: The alarm is raised when a MEP reports that either the Local or Remote loss ratio has exceeded the configured threshold for the specified remote MEP.		
Remedial action: Informational - The alarm is raised when a MEP reports that either the Local or Remote loss ratio has exceeded the configured threshold for the specified remote MEP.		

Table 39-219 DualMaster

Alarm	Attributes	Applicable major release
Name: DualMaster (420) Type: configurationAlarm Package: srrp.DualMaster Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dualMaster	Release: • N/A
Description: The alarm is raised when the local and remote SRRP instances are in the master state.		
Remedial action: Shut down one of the peer SRRP instances, modify the priority to a larger value (lower priority) and then turn it up.		

Table 39-220 duplicateAdminGroupName

Alarm	Attributes	Applicable major release
Name: duplicateAdminGroupName (4895) Type: configurationAlarm Package: svt.duplicateAdminGroupName Raised on class: svt.TunnelAdminGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateNameExists	Release: • N/A
Description: The alarm is raised when two or more global Admin Groups share the same group name.		
Remedial action: Either change the admin group name to a different value, or delete this one and recreate it with a new name.		

Table 39-221 DuplicateIpAddress

Alarm	Attributes	Applicable major release
Name: DuplicateIpAddress (5129) Type: configurationAlarm Package: rtr.DuplicateIpAddress Raised on class: rtr.VirtualRouterIpAddress	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateIpAddress	Release: • N/A
Description: The alarm is raised when a duplicate routing instance IP Address is found on two or more different NEs.		
Remedial action: Verify to ensure the duplicate routing instance IP Address is not for dual homing or network redundancy configuration. Navigate to the Virtual Router Duplicate IP Addresses listing: (Tools -> Network Resources -> Virtual Router Duplicate IP Addresses), for more information on the duplicate IP address.		

Table 39-222 DuplicateNodeIPv6SegmentId

Alarm	Attributes	Applicable major release
Name: DuplicateNodeIPv6SegmentId (11175) Type: configurationAlarm Package: isis.DuplicateNodeIPv6SegmentId Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateNodeIPv6SegmentId	Release: • N/A
Description: The alarm is raised when a duplicate node segment id value is found on two or more different NEs.		

Table 39-222 DuplicateNodeIPv6SegmentId (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify to ensure the duplicate ISIS Interface instance Node IPv6 Segment ID. Navigate to the Duplicate Node Segment Routing SID listing: (Tools -> Network Resources -> Duplicate Segment Routing SID), for more information on the duplicate Node SIDs.		

Table 39-223 DuplicateNodeSegmentId (ospf)

Alarm	Attributes	Applicable major release
Name: DuplicateNodeSegmentId (9053) Type: configurationAlarm Package: ospf.DuplicateNodeSegmentId Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateNodeSegmentId	Release: • N/A
Description: The alarm is raised when a duplicate node segment id value is found on two or more different NEs.		
Remedial action: Verify to ensure the duplicate OSPF Interface instance Node Segment ID. Navigate to the Duplicate Node Segment Routing SID listing: (Tools -> Network Resources -> Duplicate Segment Routing SID), for more information on the duplicate Node SIDs.		

Table 39-224 DuplicateNodeSegmentId (isis)

Alarm	Attributes	Applicable major release
Name: DuplicateNodeSegmentId (9053) Type: configurationAlarm Package: isis.DuplicateNodeSegmentId Raised on class: isis.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateNodeSegmentId	Release: • N/A
Description: The alarm is raised when a duplicate node segment id value is found on two or more different NEs.		
Remedial action: Verify to ensure the duplicate ISIS Interface instance Node Segment ID. Navigate to the Duplicate Node Segment Routing SID listing: (Tools -> Network Resources -> Duplicate Segment Routing SID), for more information on the duplicate Node SIDs.		

Table 39-225 DuplicateRole

Alarm	Attributes	Applicable major release
Name: DuplicateRole (470) Type: configurationAlarm Package: equipment.DuplicateRole Raised on class: equipment.StackConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: twoElementsWithSameRole	Release: • N/A
Description: The alarm is raised when a slot has the same primary or secondary role as another slot in the stack. The slot subsequently enters pass-through mode.		
Remedial action: Login to switch console, check and correct configuration and reload stack.		

Table 39-226 DuplicateRouteDistinguisher

Alarm	Attributes	Applicable major release
Name: DuplicateRouteDistinguisher (4996) Type: configurationAlarm Package: l3fwd.DuplicateRouteDistinguisher Raised on class: l3fwd.ServiceSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateRouteDistinguisher	Release: • N/A
Description: The alarm is raised if a duplicate Route Distinguisher is configured on two different NE's on different VPRN Service.		
Remedial action: The Route Distinguisher has been configured on another L3 VPRN Site. Please check the value of Route Distinguisher under Routing tab of VPRN Routing Instance.		

Table 39-227 DuplicateRouterIdProblem

Alarm	Attributes	Applicable major release
Name: DuplicateRouterIdProblem (411) Type: configurationAlarm Package: netw.DuplicateRouterIdProblem Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: duplicateRouterId	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects that the same address is being used by multiple NEs. To prevent 5620 SAM database corruption, the 5620 SAM does not discover the NE with the duplicate address.		
Remedial action: A configuration error has been made which must be corrected. Re-configure the IP address in error to a correct value.		

Table 39-228 DuplicateSlot

Alarm	Attributes	Applicable major release
Name: DuplicateSlot (468) Type: configurationAlarm Package: equipment.DuplicateSlot Raised on class: equipment.StackConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: duplicateSlotNINumber	Release: • N/A
Description: The alarm is raised when a slot has the same slot number as another stack element. The slot must relinquish its operational status because it has a higher election key, based on the up time, slot number, and MAC address. Both slots subsequently enter pass-through mode.		
Remedial action: Login to switch console, correct the slot number and reload stack.		

Table 39-229 DuplicateVrfPolicy

Alarm	Attributes	Applicable major release
Name: DuplicateVrfPolicy (229) Type: configurationAlarm Package: l3fwd.DuplicateVrfPolicy Raised on classes: • l3fwd.ServiceSiteExportPolicy • l3fwd.ServiceSiteImportPolicy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateVrfPolicyExists	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a duplicate VRF policy in a VPRN. The alarm information includes the VRF policy ID and type, and information about the service site. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has been made which must be corrected. The duplicate VRF policy must be deleted. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-230 DuplicateVrfTarget

Alarm	Attributes	Applicable major release
Name: DuplicateVrfTarget (230) Type: configurationAlarm Package: l3fwd.DuplicateVrfTarget Raised on class: l3fwd.ServiceSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateVrfTargetExists	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a duplicate VRF target in a VPRN. The alarm information includes the VRF policy ID and type, and information about the service site.		
Remedial action: A configuration error has been made which must be corrected. The duplicate VRF target must be deleted.		

Table 39-231 DyingGasp (equipment)

Alarm	Attributes	Applicable major release
Name: DyingGasp (1164) Type: communicationsAlarm Package: equipment.DyingGasp Raised on class: equipment.CardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dyingGaspSignal	Release: • N/A
Description: The alarm is raised when a Dying Gasp trap is received to indicate a power failure.		
Remedial action: This alarm is raised by the node just before going down, this might be due to the fact that the power supply connected to the node is down or failed. Please make sure the power supply to the specific node is proper.		

Table 39-232 DyingGasp (netw)

Alarm	Attributes	Applicable major release
Name: DyingGasp (1164) Type: communicationsAlarm Package: netw.DyingGasp Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dyingGasp	Release: • N/A
Description: The alarm is raised when a 7210 SAS node has loss of power.		
Remedial action: This alarm is raised by the node just before going down, this might be due to the fact that the power supply connected to the node is down or failed. Please make sure the power supply to the specific node is proper.		

Table 39-233 DyingGaspSignal

Alarm	Attributes	Applicable major release
Name: DyingGaspSignal (623) Type: communicationsAlarm Package: equipment.DyingGaspSignal Raised on class: equipment.PhysicalPort	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dyingGaspSignal	Release: • N/A
Description: The alarm is raised when a Dying Gasp signal is received from a remote 7210 SAS to indicate a power loss/from a remote node to indicate EFM-OAM is disabled on the connected remote port.		
Clearing condition: ('state' EQUAL 'Up')		
Remedial action: This alarm is raised by the node to indicate that one of the neighbouring node which is directly connected to the specific port of this node has signaled that it's going down. This might be due to the fact that the power supply connected to the remote node is down/failed or EFM-OAM is disabled. Please make sure the power supply to that specific remote node is proper or EFM-OAM on the specific remote port is enabled.		

Table 39-234 DynamicPeerLimitReached

Alarm	Attributes	Applicable major release
Name: DynamicPeerLimitReached (9030) Type: ProtocolAlarm Package: bgp.DynamicPeerLimitReached Raised on class: bgp.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: dynamicPeerLimitReached	Release: • N/A
Description: The alarm is raised when the dynamic peer limit for this BGP instance is reached.		
Remedial action: Increase the dynamic peer limit for this BGP instance.		

Table 39-235 DynSvcIdRangeConflict

Alarm	Attributes	Applicable major release
Name: DynSvcIdRangeConflict (4420) Type: DynSvcIdRangeConflict Package: dynsvc.DynSvcIdRangeConflict Raised on class: dynsvc.DynSvcNeConfig	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DynSvcIdRangeConflict	Release: • N/A
Description: The alarm is raised when the configured Dynamic Service ID Range has conflicts with one or more Range Policies.		
Remedial action: A possible conflict currently exists between the Dynamic Service ID Range specified for this NE and one or more Range Policy entries. To clear the alarm, one of the two must change. This alarm may be benign if the the conflicting Range Policy and Dynamic Service ID Range were intended.		

Table 39-236 DynSvcSapFailure

Alarm	Attributes	Applicable major release
Name: DynSvcSapFailure (4421) Type: DynSvcSapFailure Package: dynsvc.DynSvcSapFailure Raised on class: dynsvc.DynSvcNeConfig	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DynSvcSapFailure	Release: • N/A
Description: The DynSvcSapFailure alarm is raised when a Dynamic Services service SAP creation, modification or removal failed. If the SAP does not exist at the time of this notification, the value 'invalid portid' is put in the alarms sapPortId.'		
Remedial action: Ensure that the RADIUS server and python script specified by the Dynamic Service Policy is functioning correctly.		

Table 39-237 EarlyWarning (mwa)

Alarm	Attributes	Applicable major release
Name: EarlyWarning (681) Type: communicationsAlarm Package: mwa.EarlyWarning Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EarlyWarning	Release: • N/A
Description: The alarm is raised when a MPT detects an early warning event.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-238 EncapsulationTypeIncompatible

Alarm	Attributes	Applicable major release
Name: EncapsulationTypeIncompatible (250) Type: configurationAlarm Package: vll.EncapsulationTypeIncompatible Raised on class: vll.Vll	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapEncapsulationTypeIncompatible	Release: • N/A

Table 39-238 EncapsulationTypeIncompatible (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the encapsulation types of two SAPs in the same Ipipe are mismatched.		
Raising condition: ('encapsulationTypeIncompatible' EQUAL 'true')		
Clearing condition: ('encapsulationTypeIncompatible' EQUAL 'false')		
Remedial action: Ensure that the encapsulation type of any two SAPs in I-Pipe service are not mismatched.		

Table 39-239 EndpointActiveObjectChanged

Alarm	Attributes	Applicable major release
Name: EndpointActiveObjectChanged (437) Type: redundancyAlarm Package: service.EndpointActiveObjectChanged Raised on class: service.Endpoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ServiceEndpointSwitchover Applicable probable causes: • ServiceEndpointSwitchover • ForceSwitchover	Release: • N/A
Description: The alarm is raised when an automatic or manual endpoint switchover occurs.		
Remedial action: Informational - no corrective action required.		

Table 39-240 EndpointMacLimitReached

Alarm	Attributes	Applicable major release
Name: EndpointMacLimitReached (444) Type: resourceAlarm Package: vpls.EndpointMacLimitReached Raised on class: vpls.Endpoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives the svcEndpointMacLimitAlarmRaised trap from an NE, which indicates that the number of MAC addresses stored in the FDB for the endpoint exceeds the high watermark for the site FIB. The number of MAC addresses includes the static MAC addresses on the endpoint and the learned MAC addresses in the spoke SDPs that are associated with the endpoint. The alarm clears when the 5620 SAM receives the svcEndpointMacLimitAlarmCleared trap from the NE.		
Remedial action: Increase the high water mark for the site FIB to allow more entries to be added.		

Table 39-241 EPSPathDrillDownFailed

Alarm	Attributes	Applicable major release
Name: EPSPathDrillDownFailed (847) Type: EpcAlarm Package: lte.EPSPathDrillDownFailed Raised on class: lte.EPSPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPathDrillDownFailed	Release: • N/A
Description: The alarm is raised when the drilldown of an EPS path fails.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: A configuration error has been made which must be corrected. The configured drill down hint does not match the underlying transport connectivity.		

Table 39-242 EPSPathReferencedObjectDeleted

Alarm	Attributes	Applicable major release
Name: EPSPathReferencedObjectDeleted (848) Type: EpcAlarm Package: lte.EPSPathReferencedObjectDeleted Raised on class: lte.EPSPathComponent	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPathReferencedObject-Deleted	Release: • N/A
Description: The alarm is raised when a referenced object is deleted.		
Raising condition: ('componentPointer' EQUAL '\"\"')		
Clearing condition: ('componentPointer' NOT EQUAL '\"\"')		
Remedial action: Informational - no corrective action required.		

Table 39-243 EthernetPortInternalAlarm

Alarm	Attributes	Applicable major release
Name: EthernetPortInternalAlarm (3630) Type: communicationsAlarm Package: ethernetequipment.EthernetPortInternalAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortInternalAlarm	Release: • N/A
Description: The alarm is raised when an Ethernet port experiences excessive internal MAC tx errors. It is generated only when downOnInternalError is enabled on the port.		
Remedial action: This alarm indicates that the port (card) in question is likely faulty. Please replace the card with a card known to be functional.		

Table 39-244 EthernetPortRateMismatchAlarm

Alarm	Attributes	Applicable major release
Name: EthernetPortRateMismatchAlarm (8463) Type: equipmentAlarm Package: ethernetequipment.EthernetPortRateMismatchAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EthernetPortRateMisMatch	Release: • N/A
Description: The alarm is raised when an Ethernet port rate selected is not supported by SFP plugged.		
Remedial action: SFP module plugged is not compliant with the Rate configured on the interface.		

Table 39-245 EthernetTunnelDown

Alarm	Attributes	Applicable major release
Name: EthernetTunnelDown (771) Type: configurationAlarm Package: ethernettunnel.EthernetTunnelDown Raised on class: ethernettunnel.EthernetTunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetTunnelDown	Release: • N/A
Description: The alarm is raised when the aggregated Ethernet tunnel Operational State is Down.		
Raising condition: (('aggrEndPtOperationalState' EQUAL 'Down'))		
Clearing condition: (('aggrEndPtOperationalState' NOT EQUAL 'Down'))		
Remedial action: Fix the error indicated in the alarm, e.g. port down, MEP down...		

Table 39-246 EventsThrottled

Alarm	Attributes	Applicable major release
Name: EventsThrottled (356) Type: communicationsAlarm Package: netw.EventsThrottled Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: snmpDaemonOverloaded	Release: • N/A
Description: The alarm is raised when an NE throttles events because the event rate exceeds the configured maximum.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation on the NE is required to understand what is causing the consistently high rate of event traffic.		

Table 39-247 ExcessiveEnvironmentTemparature (mwa)

Alarm	Attributes	Applicable major release
Name: ExcessiveEnvironmentTemparature (1118) Type: environmentalAlarm Package: mwa.ExcessiveEnvironmentTemparature Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ExcessiveEnvironmentTem-parature	Release: • N/A
Description: This alarm is raised when a MPT detects excessive environmental temperature.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-248 ExportPolicyNotFound

Alarm	Attributes	Applicable major release
Name: ExportPolicyNotFound (231) Type: configurationAlarm Package: l3fwd.ExportPolicyNotFound Raised on class: l3fwd.ServiceSiteExportPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: exportPolicyDoesNotExist	Release: • N/A
Description: The alarm is raised when a VRF export policy for a VPRN cannot be found. The alarm information includes the policy ID. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has occurred which must be corrected. The VRP export policy must be created and distributed to the NE reporting the problem. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-249 ExternalLinkDown

Alarm	Attributes	Applicable major release
Name: ExternalLinkDown (9014) Type: communicationsAlarm Package: optical.ExternalLinkDown Raised on class: optical.OpticalLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when any end point of the external Optical Link is operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the Link End points to understand why the underlying transport network is unreliable.		

Table 39-250 FailureToSwitchManagementProtocol

Alarm	Attributes	Applicable major release
Name: FailureToSwitchManagementProtocol (1076) Type: communicationsAlarm Package: netw.FailureToSwitchManagementProtocol Raised on class: netw.NodeDiscoveryControl	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: managementAddressInvalid	Release: • N/A

Table 39-250 FailureToSwitchManagementProtocol (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM cannot switch the management address of an NE from one IP version to another.		
Remedial action: The additional text field of the alarm will provide guidance as to the reason for the failure - the most probable cause is a configuration error. The configuration error must be corrected. Once the issue has been resolved SAM will automatically re-attempt.		

Table 39-251 FanFailure (mwa)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: mwa.FanFailure Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanFailure	Release: • N/A
Description: This alarm is raised when a MPT detects a fan failure.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-252 FanRPMAlarm

Alarm	Attributes	Applicable major release
Name: FanRPMAlarm (1126) Type: equipmentAlarm Package: equipment.FanRPMAlarm Raised on class: equipment.Fan	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fanFailure	Release: • N/A
Description: The alarm is raised when a fan alarm usage state is other than Normal.		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 39-253 fgwConfigurationUpdateFailed

Alarm	Attributes	Applicable major release
Name: fgwConfigurationUpdateFailed (9020) Type: communicationsAlarm Package: femto.fgwConfigurationUpdateFailed Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • N/A
Description: This alarm indicates that the New Configuration Update on FGW Node is Failed.		
Remedial action: Not available		

Table 39-254 FGWFileTransferFailure

Alarm	Attributes	Applicable major release
Name: FGWFileTransferFailure (11824) Type: communicationsAlarm Package: femto.FGWFileTransferFailure Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • N/A
Description: This alarm indicates that there was a failure in File transfer Operation with FGW.		
Remedial action: Check The Communication Link and/or SSH Key-sharing between SAM and FGW.This Notification may be required by Global Product support for Debugging purpose		

Table 39-255 FIBHighOccupancy

Alarm	Attributes	Applicable major release
Name: FIBHighOccupancy (752) Type: resourceAlarm Package: equipment.FIBHighOccupancy Raised on class: equipment.BaseCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FIBHighOccupancy	Release: • N/A
Description: The alarm is raised when the FIB occupancy on an IOM card changes from normal to high.		
Remedial action: Informational - no corrective action required.		

Table 39-256 FibOutOfSynch

Alarm	Attributes	Applicable major release
Name: FibOutOfSynch (625) Type: resourceAlarm Package: equipment.FibOutOfSynch Raised on class: equipment.DaughterCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fibUpdateFailed	Release: • N/A
Description: The alarm is raised when the FIB on an MDA is out of synchronization.		
Remedial action: Informational - no corrective action required.		

Table 39-257 FileTransferFailure

Alarm	Attributes	Applicable major release
Name: FileTransferFailure (8152) Type: communicationsAlarm Package: netw.FileTransferFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • N/A

Table 39-257 FileTransferFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SAM cannot transfer a file from a Network Element due to one or more of the following causes: unreachable NE, remote file not found, authentication failure, file transfer interrupted, or lack of available local storage space.		
Remedial action: Investigation is required to resolve the following possible scenarios: SAM server has connectivity issue with NE; insufficient disk space on the SAM server to accommodate the file transfer being attempted; loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues. If SAM implements recovery mechanism for the target node, check the file's target directory to confirm whether the file has already been recovered.		

Table 39-258 FilterApplyPathProblem

Alarm	Attributes	Applicable major release
Name: FilterApplyPathProblem (4904) Type: configurationAlarm Package: filterprefixlist.FilterApplyPathProblem Raised on class: filterprefixlist.PrefixListApplyPathMember	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tFilterApplyPathProblem	Release: • N/A
Description: The alarm is raised when a problem is encountered for a configured IP PrefixList apply-path rule.		
Remedial action: Clear the alarm and verify the prefix-list configurations which might have reached the maximum limit. Try reducing the prefix-list/ apply-path members.		

Table 39-259 FilterEmbeddingOperStateChange

Alarm	Attributes	Applicable major release
Name: FilterEmbeddingOperStateChange (4973) Type: configurationAlarm Package: aclfilter.FilterEmbeddingOperStateChange Raised on class: aclfilter.FilterEmbeddedRefTable	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tFilterEmbeddingOperStat-eChange	Release: • N/A
Description: The alarm is raised when the embedding oper state change is other than in-service.		
Remedial action: The alarm is raised when the embedded filter operstate is other than inService. Remove and reapply the embedding to make operstate as inService.		

Table 39-260 FirmwareDownloadOnGoing (equipment)

Alarm	Attributes	Applicable major release
Name: FirmwareDownloadOnGoing (626) Type: equipmentAlarm Package: equipment.FirmwareDownloadOnGoing Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: firmwareDownloadOnGoing	Release: • N/A
Description: The alarm is raised when a firmware download is in progress.		

Table 39-260 FirmwareDownloadOnGoing (equipment) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - Firmware for the equipment is downloading.		

Table 39-261 FirmwareMismatchAlarm

Alarm	Attributes	Applicable major release
Name: FirmwareMismatchAlarm (146) Type: firmwareAlarm Package: equipment.FirmwareMismatchAlarm Raised on class: equipment.Card	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootRomVersionMismatch Applicable probable causes: • bootRomVersionMismatch • fpgaVersionMismatch	Release: • N/A
Description: The alarm is raised when a device detects a mismatch between the firmware version and the device software image. The alarm information includes the expected firmware version.		
Remedial action: Either the firmware or the device SW must be upgraded to compatible versions. The image (firmware or device SW) which is the oldest should be upgraded. Firmware must be upgraded using the NE's CLI. 5620 SAM can be used to upgrade the SW image on the device.		

Table 39-262 FirmwareUpgradeAlarm

Alarm	Attributes	Applicable major release
Name: FirmwareUpgradeAlarm (212) Type: firmwareAlarm Package: equipment.FirmwareUpgradeAlarm Raised on class: equipment.Card	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: firmwareUpgraded	Release: • N/A
Description: The alarm is raised when a device automatically upgrades the firmware of a hot-inserted IOM or CPM.		
Remedial action: Informational - no corrective action required.		

Table 39-263 firstExpirationThresholdCrossed

Alarm	Attributes	Applicable major release
Name: firstExpirationThresholdCrossed (2907) Type: configurationAlarm Package: ranlicense.firstExpirationThresholdCrossed Raised on class: ranlicense.RANLicense	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ageingLicense	Release: • N/A
Description: The alarm is raised when the specified First Expiration Threshold for RAN licensing is crossed.		
Remedial action: Ask for a new LKDI license file with a further expiration date.		

Table 39-264 firstUsageThresholdCrossed

Alarm	Attributes	Applicable major release
Name: firstUsageThresholdCrossed (2908) Type: configurationAlarm Package: ranlicense.firstUsageThresholdCrossed Raised on class: ranlicense.RANLicense	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: insufficientPurchasedLicenses	Release: • N/A
Description: The alarm is raised when the specified First Usage Threshold for RAN licensing is crossed.		
Remedial action: Ask for a new LKDI license file with more tokens.		

Table 39-265 FlowRouteInvalid

Alarm	Attributes	Applicable major release
Name: FlowRouteInvalid (2932) Type: ProtocolAlarm Package: bgp.FlowRouteInvalid Raised on class: bgp.Peer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: flowRouteInvalid	Release: • N/A
Description: The alarm is raised when the received BGP flow route is invalid. The BGP peer dose not create ip filter entry for the received flow route.		
Remedial action: The NE has received an invalid flow route from a 3rd party appliance which is monitoring the network for suspect traffic. This could be the result of corruption or a SW error on the 3rd party appliance. Please refer to the documentation supplied with appliance for assistance.		

Table 39-266 FlowspecUnsupportdComAction

Alarm	Attributes	Applicable major release
Name: FlowspecUnsupportdComAction (2933) Type: ProtocolAlarm Package: bgp.FlowspecUnsupportdComAction Raised on class: bgp.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unsupportdComAction	Release: • N/A
Description: The alarm is raised when the best route for a FlowSpec NLRI is received from a remote BGP peer with an extended community action that is unsupported.		
Remedial action: Informational - no corrective action required.		

Table 39-267 ForceQTagForwardingMisconfiguration (epipe)

Alarm	Attributes	Applicable major release
Name: ForceQTagForwardingMisconfiguration (813) Type: configurationAlarm Package: epipe. ForceQTagForwardingMisconfiguration Raised on class: epipe.Epipe	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: forceQTagForwardingInconsis-tent	Release: • N/A
Description: The alarm is raised when two I-sites in a service use different Force Q Tag Forwarding values.		
Raising condition: ('operationalFlags'anyBit'Force Q Tag Forwarding Inconsistent')		
Clearing condition: NOT (('operationalFlags'anyBit'Force Q Tag Forwarding Inconsistent'))		
Remedial action: Check configuration so that I-sites in the service use same Force Q-Tag Forwarding values.		

Table 39-268 ForceQTagForwardingMisconfiguration (vpls)

Alarm	Attributes	Applicable major release
Name: ForceQTagForwardingMisconfiguration (813) Type: configurationAlarm Package: vpls.ForceQTagForwardingMisconfiguration Raised on class: vpls.AbstractVpls	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: forceQTagForwardingInconsis-tent	Release: • N/A
Description: The alarm is raised when two I-sites in a service use different Force Q Tag Forwarding values.		
Raising condition: ('operationalFlags'anyBit'Force Q Tag Forwarding Inconsistent')		
Clearing condition: NOT (('operationalFlags'anyBit'Force Q Tag Forwarding Inconsistent'))		
Remedial action: Check configuration so that I-sites in the service use same Force Q-Tag Forwarding values.		

Table 39-269 FrameSizeProblem (service)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: service.FrameSizeProblem Raised on class: service.Service	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • N/A
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: ('mtuInconsistent' EQUAL 'true')		
Clearing condition: ('mtuInconsistent' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 39-270 FtpClientFailure

Alarm	Attributes	Applicable major release
Name: FtpClientFailure (357) Type: communicationsAlarm Package: netw.FtpClientFailure Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ftpClientFailure	Release: • N/A
Description: The alarm is raised when an NE sends notification that an FTP operation initiated by the FTP client fails because of file unavailability, interruption during the file transfer, or a lack of available storage space.		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space on the NE to accommodate the file transfer being attempted; the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 39-271 FTPLoginMaxAttempts

Alarm	Attributes	Applicable major release
Name: FTPLoginMaxAttempts (10267) Type: communicationsAlarm Package: netw.FTPLoginMaxAttempts Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FtpLoginMaxAttempts	Release: • N/A
Description: The alarm is raised when the number of ftp login failures due to incorrect user name or password using SSH session exceeds the configured value.		
Remedial action: The wrong password was entered by the user during FTP. Please try to log in again later.		

Table 39-272 GlobalAppProfileCreated

Alarm	Attributes	Applicable major release
Name: GlobalAppProfileCreated (2931) Type: ConfigurationAlarm Package: aapolicy.GlobalAppProfileCreated Raised on class: aapolicy.ApplicationProfile	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: globalAppProfileMissing	Release: • N/A
Description: The alarm is raised when a global application profile to which a global transit IP policy is referenced does not exist. The alarm notifies the user that a global application profile has been created.		
Remedial action: Informational. A global Application Profile has been created; this object is referenced by a Transit IP Policy or Transit Prefix Policy.		

Table 39-273 globalLicenseViolation

Alarm	Attributes	Applicable major release
Name: globalLicenseViolation (2909) Type: configurationAlarm Package: ranlicense.globalLicenseViolation Raised on class: ranlicense.RANLicenseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: atLeastOneLicenseInViolation	Release: • N/A
Description: The alarm is raised when at least one RAN license is in violation.		
Remedial action: Provide a new LKDI license file with a further expiration date and/or more tokens.		

Table 39-274 GneCommunicationAlarm

Alarm	Attributes	Applicable major release
Name: GneCommunicationAlarm (783) Type: CommunicationAlarm Package: netw.GneCommunicationAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-275 GneEnvironmentalAlarm

Alarm	Attributes	Applicable major release
Name: GneEnvironmentalAlarm (784) Type: EnvironmentalAlarm Package: netw.GneEnvironmentalAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-276 GneEquipmentAlarm

Alarm	Attributes	Applicable major release
Name: GneEquipmentAlarm (785) Type: EquipmentAlarm Package: netw.GneEquipmentAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A

Table 39-276 GneEquipmentAlarm (continued)

Alarm	Attributes	Applicable major release
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-277 GneInterfaceAlarm

Alarm	Attributes	Applicable major release
Name: GneInterfaceAlarm (9610) Type: EquipmentAlarm Package: genericne.GneInterfaceAlarm Raised on class: genericne.GenericNeInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-278 GneMTIEAlarm (netw)

Alarm	Attributes	Applicable major release
Name: GneMTIEAlarm (3633) Type: EquipmentAlarm Package: netw.GneMTIEAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-279 GneMTIEAlarm (genericne)

Alarm	Attributes	Applicable major release
Name: GneMTIEAlarm (3633) Type: EquipmentAlarm Package: genericne.GneMTIEAlarm Raised on class: genericne.GenericNeInterface	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		

Table 39-279 GneMTIEAlarm (genericne) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-280 GneProcessingErrorAlarm

Alarm	Attributes	Applicable major release
Name: GneProcessingErrorAlarm (786) Type: ProcessingErrorAlarm Package: netw.GneProcessingErrorAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-281 GneQualityOfServiceAlarm

Alarm	Attributes	Applicable major release
Name: GneQualityOfServiceAlarm (787) Type: QualityOfServiceAlarm Package: netw.GneQualityOfServiceAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-282 GneServiceAlarm

Alarm	Attributes	Applicable major release
Name: GneServiceAlarm (788) Type: ServiceAlarm Package: netw.GneServiceAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-283 GneSystemAlarm

Alarm	Attributes	Applicable major release
Name: GneSystemAlarm (789) Type: SystemAlarm Package: netw.GneSystemAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-284 GneTransportAlarm

Alarm	Attributes	Applicable major release
Name: GneTransportAlarm (790) Type: TransportAlarm Package: netw.GneTransportAlarm Raised on class: netw.NetworkElement	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: User_Defined	Release: • N/A
Description: This user-definable alarm is raised against a generic NE when the 5620 SAM receives a trap from the generic NE that is mapped to the alarm in a generic NE alarm catalogue. The alarm mapping defines the Probable cause, Severity, and Implicitly cleared values, and optionally contains an extension that is appended to the Name value.		
Remedial action: This alarm is mapped from a GNE trap. Remedial action depends on the specific equipment and trap definition.		

Table 39-285 GponPortInBandAlarm

Alarm	Attributes	Applicable major release
Name: GponPortInBandAlarm (3697) Type: gponInBandSignallingAlarm Package: equipment.GponPortInBandAlarm Raised on class: equipment.GponPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandSignallingNotEstablishedBetweenSARAndONT	Release: • N/A
Description: The alarm is raised when in-band signaling between the ONT and SAR for GPON statistics collection is not established after 30 seconds of GPON port uptime.		
Remedial action: Informational - Reachability between SAR and ONT devices has to be checked.		

Table 39-286 GponPortInBandAlarmClear

Alarm	Attributes	Applicable major release
Name: GponPortInBandAlarmClear (3698) Type: gponInBandSignallingAlarm Package: equipment.GponPortInBandAlarmClear Raised on class: equipment.GponPortSpecifics	Severity: cleared Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InBandSignallingEstablished-BetweenSARAndONT	Release: • N/A
Description: The alarm is raised when in-band signaling between the ONT and SAR for GPON statistics collection is established.		
Remedial action: Informational - no corrective action required.		

Table 39-287 GroupInSSMRange

Alarm	Attributes	Applicable major release
Name: GroupInSSMRange (187) Type: configurationAlarm Package: pim.GroupInSSMRange Raised on class: pim.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: STARGGroupInSSMRange	Release: • N/A
Description: The alarm is raised when an NE receives a PIM register, PIM (*,G) assert, PIM (*,G) join/prune, or an IGMP local membership message for a group defined in the SSM address range.		
Remedial action: Informational - no corrective action required		

Table 39-288 GwAcrFailuresAlarmMajor

Alarm	Attributes	Applicable major release
Name: GwAcrFailuresAlarmMajor (2955) Type: communicationsAlarm Package: lte.GwAcrFailuresAlarmMajor Raised on class: lte.AgwRfPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: connectionDown	Release: • N/A
Description: A tmnxMobGwAcrFailuresAlarmMajor is generated when 2 ACR transmission failures occur in a 10 second interval or 5 ACR transmission failures occur in a 60 second interval to the peer.		
Remedial action: Informational - a threshold for Anonymous Communication Rejection transmission failures has been exceeded. If the condition persists please contact your Nokia support representative for assistance.		

Table 39-289 GwDdnThrottlingStart

Alarm	Attributes	Applicable major release
Name: GwDdnThrottlingStart (4630) Type: communicationsAlarm Package: lte.GwDdnThrottlingStart Raised on class: lte.SigAGWGTPPMIPPeer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: downLinkThrottling	Release: • N/A

Table 39-289 GwDdnThrottlingStart (continued)

Alarm	Attributes	Applicable major release
Description: A GwDdnThrottlingStart notification is generated when the serving gateway (SGW) starts throttling the Downlink Data Notification (DDN) for the low priority traffic towards a peer node (SGSN/MME).		
Remedial action: The serving gateway (SGW) starts throttling the Downlink Data Notification (DDN) for the low priority traffic towards a peer node (SGSN/MME). When the throttling duration is passed, the SGW will stop throttling the DDN.		

Table 39-290 GwDdnThrottlingStop

Alarm	Attributes	Applicable major release
Name: GwDdnThrottlingStop (4631) Type: communicationsAlarm Package: lte.GwDdnThrottlingStop Raised on class: lte.SigAGWGTPPMIPPeer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: downLinkThrottling	Release: • N/A
Description: A GwDdnThrottlingStop notification is generated when the serving gateway (SGW) stops throttling the Downlink Data Notification (DDN) for the low priority traffic towards a peer node (SGSN/MME).		
Remedial action: The serving gateway (SGW) stops throttling the Downlink Data Notification (DDN) for the low priority traffic towards a peer node (SGSN/MME). When another throttling instruction is received from a peer node, the SGW will start throttling the DDN.		

Table 39-291 GwPoolCapacityAlarmMajor

Alarm	Attributes	Applicable major release
Name: GwPoolCapacityAlarmMajor (5190) Type: EpcAlarm Package: lte.GwPoolCapacityAlarmMajor Raised on class: lte.IpPool	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Threshold	Release: • N/A
Description: A tmnxMobGwPoolCapacityAlarmMajor notification is generated when either the IPv4 or IPv6 address pool usage reaches 95% of the pool size.		
Remedial action: The IPv4 or IPv6 address pool usage reached 95% of the pool size. Need to look at increasing the address pool size.		

Table 39-292 GwPoolCapacityAlarmMinor

Alarm	Attributes	Applicable major release
Name: GwPoolCapacityAlarmMinor (5191) Type: EpcAlarm Package: lte.GwPoolCapacityAlarmMinor Raised on class: lte.IpPool	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Threshold	Release: • N/A
Description: A tmnxMobGwPoolCapacityAlarmMinor notification is generated when either the IPv4 or IPv6 address pool usage reaches 85% of the pool size.		

Table 39-292 GwPoolCapacityAlarmMinor (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational: The IPv4 or IPv6 address pool usage reached 85% of the pool size. Need to closely monitor the usage.		

Table 39-293 HardwareBootFailure

Alarm	Attributes	Applicable major release
Name: HardwareBootFailure (108) Type: softwareAlarm Package: sw.HardwareBootFailure Raised on class: sw.CardSoftware	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareBootProblemDueTo-HardwareIssues	Release: • N/A
Description: The alarm is raised when an NE fails to boot because of a hardware problem.		
Remedial action: Please contact your Nokia support representative for assistance.		

Table 39-294 HardwareRedundancyAlarm

Alarm	Attributes	Applicable major release
Name: HardwareRedundancyAlarm (147) Type: equipmentAlarm Package: equipment.HardwareRedundancyAlarm Raised on class: equipment.ControlProcessor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryCpmFailure	Release: • N/A
Description: The alarm is raised when the primary CPM fails.		
Remedial action: The CPM card in the chassis may have suffered a failure. Remove and reset the card in question. If this does not resolve the problem replace the card.		

Table 39-295 HashLabelMismatch (svt)

Alarm	Attributes	Applicable major release
Name: HashLabelMismatch (1113) Type: configurationAlarm Package: svt.HashLabelMismatch Raised on class: svt.SdpBinding	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: hashLabelMismatch	Release: • N/A
Description: The alarm is raised when an SDP binding hash label is enabled and the return SDP binding hash label is disabled. If this misconfiguration causes the mismatch of the operational hash label on both sides, the receiving site will drop the data packets as a result. This alarm is cleared when the hash label is either enabled or disabled on both sides.		
Remedial action: The hash label must be enabled or disabled on both ends of the SDP		

Table 39-296 HashLabelMismatch (vprn)

Alarm	Attributes	Applicable major release
Name: HashLabelMismatch (1113) Type: configurationAlarm Package: vprn.HashLabelMismatch Raised on class: vprn.Vprn	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: hashLabelMismatch	Release: • N/A
Description: The alarm is raised when the hash label is enabled on a VPRN site and disabled on another site in the service.		
Remedial action: A configuration error has occurred which must be corrected. The hash label must be enabled or disabled on both ends of the SDP		

Table 39-297 HashLabelSignalCapabilityMismatch

Alarm	Attributes	Applicable major release
Name: HashLabelSignalCapabilityMismatch (3327) Type: configurationAlarm Package: svt.HashLabelSignalCapabilityMismatch Raised on class: svt.SdpBinding	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: hashLabelSignalCapabili-tyMismatch	Release: • N/A
Description: The alarm is raised when an SDP binding hash label signal capability is enabled and the return SDP binding hash label signal capability is disabled or not supported. If this misconfiguration causes the mismatch of the operational hash label on both sides, the receiving site will drop the data packets as a result. This alarm is cleared when the hash label signal capability is either enabled or disabled on both sides.		
Remedial action: The hash label signal capability must be enabled or disabled on both ends of the SDP		

Table 39-298 HDMConfiguration_FileserverHostNameForFemtoConfigurationAlarm

Alarm	Attributes	Applicable major release
Name: HDMConfiguration_ FileserverHostNameForFemtoConfigurationAlarm (11148) Type: configurationAlarm Package: femto.HDMConfiguration_ FileserverHostNameForFemtoConfigurationAlarm Raised on class: femto.HDMConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The fileserverHostNameForFemto is not configured.		
Remedial action: Configure the FileserverHostNameForFemto in Smallcell Configuration window.		

Table 39-299 HDMConfiguration_OamNeIPConfigurationAlarm

Alarm	Attributes	Applicable major release
Name: HDMConfiguration_ OamNeIPConfigurationAlarm (11149) Type: configurationAlarm Package: femto.HDMConfiguration_ OamNeIPConfigurationAlarm Raised on class: femto.HDMConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The oamNeIP is not configured.		
Remedial action: Configure the OamNeIPAddress in Smallcell Configuration window.		

Table 39-300 HighBER (mwa)

Alarm	Attributes	Applicable major release
Name: HighBER (682) Type: communicationsAlarm Package: mwa.HighBER Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBER	Release: • N/A
Description: The alarm is raised when a MPT detects a high BER.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-301 HighBER (equipment)

Alarm	Attributes	Applicable major release
Name: HighBER (682) Type: communicationsAlarm Package: equipment.HighBER Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: highBER	Release: • N/A
Description: The alarm is raised when an MSS detects a high BER.		
Remedial action: 1. Retrieve power level reading on the local OT port.2. Clean the fiber.3. If cleaning the fiber does not clear the problem, replace the fiber.4. If the power level is within the operating range, check for pluggable module alarms.5. Replace the pluggable module.		

Table 39-302 HighLevelRoutesReached

Alarm	Attributes	Applicable major release
Name: HighLevelRoutesReached (1197) Type: ProtocolAlarm Package: l3fwd.HighLevelRoutesReached Raised on class: l3fwd.ServiceSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighLevelRoutesReached	Release: • N/A

Table 39-302 HighLevelRoutesReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of routes in a VPRN exceeds the high threshold value. The high threshold value is a percentage of the maximum number of routes specified in the VPRN configuration. The percentage is derived by adding 100 to the threshold value in the VPRN configuration and dividing the result by 2. The alarm information includes the number of routes and this calculated high threshold value.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE or VRF instance in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-303 HistCorrDbSizeThresholdExceeded

Alarm	Attributes	Applicable major release
Name: HistCorrDbSizeThresholdExceeded (5169) Type: configurationAlarm Package: histcorr.HistCorrDbSizeThresholdExceeded Raised on class: histcorr.HistCorrPartitionManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HistCorrEventDBSizeIsNot-Sufficient	Release: • N/A
Description: The alarm is raised when the actual DB size consumed by Correlation Events exceeds the threshold.		
Remedial action: Correlation Events DB storage reached threshold or exceeded, increase "Max DB Size" in Correlation Partition Manager GUI.		

Table 39-304 HoldTimeInconsistent

Alarm	Attributes	Applicable major release
Name: HoldTimeInconsistent (810) Type: ProtocolAlarm Package: bgp.HoldTimeInconsistent Raised on class: bgp.Peer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: holdTimeInconsistent	Release: • N/A
Description: The alarm is raised when a BGP site tries to establish a peering using a hold time that is less than the configured strict hold time. The peering is rejected as a result.		
Remedial action: A configuration error has occurred which must be corrected. The hold time must be set to a value greater than the strict hold time.		

Table 39-305 HOPathUnequipped

Alarm	Attributes	Applicable major release
Name: HOPathUnequipped (9006) Type: communicationsAlarm Package: tdm.HOPathUnequipped Raised on class: tdm.AUn	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UNEQP	Release: • N/A
Description: The alarm is raised on HOPath Unequipped (NEND).		
Remedial action: HO Path is unequipped at NEND.		

Table 39-306 HostBGPPeeringSetupFailed

Alarm	Attributes	Applicable major release
Name: HostBGPPeeringSetupFailed (9592) Type: processingErrorAlarm Package: service.HostBGPPeeringSetupFailed Raised on class: service.ServiceAccessPoint	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: HostBGPPeeringSetupFailed	Release: • N/A
Description: The alarm indicates that the system was unable to create a BGP neighbor and set up BGP peering for the given host. This alarm is related to the NE trap sapHostBGPPeeringSetupFailed.		
Remedial action: Please verify BGP peering attributes and ensure configuration is correct. The recovery action depends on the specific cause of failure. Please review the alarm's additional text for further details.		

Table 39-307 HostnameMismatch

Alarm	Attributes	Applicable major release
Name: HostnameMismatch (732) Type: configurationAlarm Package: server.HostnameMismatch Raised on class: server.SamServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hostnameMismatch	Release: • N/A
Description: The alarm is raised when an auxiliary or standby server host name in a 5620 SAM main server configuration does not match the host name of the auxiliary or standby server /etc/hosts file.		
Remedial action: A configuration error has been made which must be corrected. The standby SAM server or AUX server host names on the 5620 SAM server are not resolving correctly and must be corrected (i.e. in the /etc/hosts file).		

Table 39-308 HostPortReachabilityDown

Alarm	Attributes	Applicable major release
Name: HostPortReachabilityDown (10274) Type: virtualPortAlarm Package: dctr.HostPortReachabilityDown Raised on class: dctr.GatewayVirtualPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HostPortPrefixMissing	Release: • N/A

Table 39-308 HostPortReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when Host type VP is reachability down.		
Raising condition: (('bgpReachabilityState' EQUAL '2') AND ('vpType' EQUAL '1') AND ('isRedundant' EQUAL 'false'))		
Clearing condition: (('vpType' EQUAL '1'))		
Remedial action: This alarm can be cleared when host type virtual port BGP prefix is up.		

Table 39-309 HostSharedFilterHighWatermarkAlarm

Alarm	Attributes	Applicable major release
Name: HostSharedFilterHighWatermarkAlarm (4974) Type: configurationAlarm Package: aclfilter. HostSharedFilterHighWatermarkAlarm Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HostSharedFilterHighWatermarkAlarm	Release: • N/A
Description: The alarm is raised when the number of dynamically allocated Host Shared Filters based on the indicated filter reaches or exceeds the configured high watermark. This alarm is cleared when the number of dynamically allocated Host Shared Filters drops to or below the configured low watermark of the indicated filter.		
Remedial action: Please check the watermark configurations on the indicated filter and make an adjustment accordingly.		

Table 39-310 IgmpGrpIfSapMaxGroupsLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpGrpIfSapMaxGroupsLimitExceeded (3979) Type: configurationAlarm Package: igmp. IgmpGrpIfSapMaxGroupsLimitExceeded Raised on class: igmp.GroupInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpGrpIfSapMaxGroupsLimitExceeded	Release: • N/A
Description: This alarm is raised when an IGMP host subscribes to a new multicast group that cannot be installed because the maximum number of active groups on the IGMP group interface SAP has already been reached.		
Remedial action: Increase the value of the 'maxGroups' attribute in the parent IGMP group interface so that the number of active IGMP groups stays under the configured threshold.		

Table 39-311 IgmpGrpIfSapMaxGrpSrcLimExcd

Alarm	Attributes	Applicable major release
Name: IgmpGrpIfSapMaxGrpSrcLimExcd (4622) Type: configurationAlarm Package: igmp.IgmpGrpIfSapMaxGrpSrcLimExcd Raised on class: igmp.GroupInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpGrpIfSapMaxGrpSr-cLimExcd	Release: • N/A
Description: This alarm is raised when an attempt is made to configure a group source for a group when the number of group sources is equal to vRtrIgmpGrpIfSapMaxGrpSources, the maximum number of group sources per group supported on the SAP.		
Remedial action: Increase the value of the 'maxGrpSources' attribute in the parent IGMP group interface so that the number of active IGMP Group sources stays under the configured threshold.		

Table 39-312 IgmpGrpIfSapMaxSourcesLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpGrpIfSapMaxSourcesLimitExceeded (3980) Type: configurationAlarm Package: igmp. IgmpGrpIfSapMaxSourcesLimitExceeded Raised on class: igmp.GroupInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpGrpIfSapMax-SourcesLimitExceeded	Release: • N/A
Description: This alarm is raised when an IGMP host subscribes to a multicast group with a source that cannot be installed because the maximum number of active sources on the IGMP group interface SAP has already been reached.		
Remedial action: Increase the value of the 'maxSources' attribute in the parent IGMP group interface so that the number of active IGMP sources stays under the configured threshold.		

Table 39-313 IgmpHostMaxGrpSrcsLimitExcd

Alarm	Attributes	Applicable major release
Name: IgmpHostMaxGrpSrcsLimitExcd (4623) Type: configurationAlarm Package: igmp.IgmpHostMaxGrpSrcsLimitExcd Raised on class: igmp.GrpInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpHostMaxGrpSrcsLimit-Excd	Release: • N/A
Description: This alarm is raised when an attempt is made to configure a source for a group when the number of group sources is equal to vRtrIgmpHostMaxGrpSources, the maximum number of group sources per group supported on the host.		
Remedial action: Increase the value of the 'maxGrpSources' attribute in the parent IGMP group interface so that the number of active IGMP Group sources stays under the configured threshold.		

Table 39-314 IgmpSnpgGrpDroppedLimitExceeded (svt)

Alarm	Attributes	Applicable major release
Name: IgmpSnpgGrpDroppedLimitExceeded (392) Type: SdpBindingAlarm Package: svt.IgmpSnpgGrpDroppedLimitExceeded Raised on class: svt.SdpBindingIgmpSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxN-brGrpsReached	Release: • N/A
Description: The alarm is raised when an IGMP group is removed from an SDP binding because the number of allowed IGMP groups specified by sdpBndIgmpSnpgCfgMaxNbrGrps is reached.		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP groups on the SDP.		

Table 39-315 IgmpSnpgGrpDroppedLimitExceeded (vpls)

Alarm	Attributes	Applicable major release
Name: IgmpSnpgGrpDroppedLimitExceeded (392) Type: AccessInterfaceAlarm Package: vpls.IgmpSnpgGrpDroppedLimitExceeded Raised on class: vpls.L2AccessInterfaceIgmpSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxN-brGrpsReached	Release: • N/A
Description: The alarm is raised when an IGMP group is removed from a SAP because the number of allowed IGMP groups specified by sapIgmpSnpgCfgMaxNbrGrps is reached.		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP groups on the SAP.		

Table 39-316 IgmpSnpgGrpSrcLimitExceed

Alarm	Attributes	Applicable major release
Name: IgmpSnpgGrpSrcLimitExceed (4894) Type: SdpBindingAlarm Package: svt.IgmpSnpgGrpSrcLimitExceed Raised on class: svt.SdpBindingIgmpSnpgCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IgmpSnpgGrpSrcLimitExceed	Release: • N/A
Description: The alarm is raised when an IGMP group or source is dropped on a given SDP Bind because a user configurable upper limit given by sdpBndIgmpSnpgCfgMaxNbrGrpSrcs is reached		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP group sources on the SDP.		

Table 39-317 IgmpSnpgGrpSrcLimitExceeded

Alarm	Attributes	Applicable major release
Name: IgmpSnpgGrpSrcLimitExceeded (4897) Type: AccessInterfaceAlarm Package: vpls.IgmpSnpgGrpSrcLimitExceeded Raised on class: vpls.L2AccessInterfaceIgmpSnpgCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxNbrGrpSrcsReached	Release: • N/A
Description: The alarm is raised when an IGMP group or source is dropped on a given SAP because a user configurable upper limit given by sapIgmpSnpgCfgMaxNbrGrpSrcs is reached		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP Group sources on the SAP.		

Table 39-318 IgmpSnpgSrcDroppedLimitExceeded (svt)

Alarm	Attributes	Applicable major release
Name: IgmpSnpgSrcDroppedLimitExceeded (735) Type: SdpBindingAlarm Package: svt.IgmpSnpgSrcDroppedLimitExceeded Raised on class: svt.SdpBindingIgmpSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxNbrSrcsReached	Release: • N/A
Description: The alarm is raised when an IGMP source is removed from an SDP binding because the number of allowed IGMP sources specified by sdpBndIgmpSnpgCfgMaxNbrSrcs is reached.		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP sources on the SDP.		

Table 39-319 IgmpSnpgSrcDroppedLimitExceeded (vpls)

Alarm	Attributes	Applicable major release
Name: IgmpSnpgSrcDroppedLimitExceeded (735) Type: AccessInterfaceAlarm Package: vpls.IgmpSnpgSrcDroppedLimitExceeded Raised on class: vpls.L2AccessInterfaceIgmpSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxNbrSrcsReached	Release: • N/A
Description: The alarm is raised when an IGMP source is removed from a SAP because the number of allowed IGMP sources specified by sapIgmpSnpgCfgMaxNbrGrps is reached.		
Remedial action: This can be remedied by increasing the maximum number of allowed IGMP sources on the SAP.		

Table 39-320 ignoreUnknownImportedLicenses

Alarm	Attributes	Applicable major release
Name: ignoreUnknownImportedLicenses (2910) Type: configurationAlarm Package: ranlicense.ignoreUnknownImportedLicenses Raised on class: ranlicense.RANLicenseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licenseMappingFileNo-tAlignedWithImportedFile	Release: • N/A
Description: The alarm is raised when at least one of the imported licenses in the LKDI license file is not recognized by the 5620 SAM.		
Remedial action: Informational - Provide a LKDI license file compliant with supported licenses.		

Table 39-321 ImportPolicyNotFound

Alarm	Attributes	Applicable major release
Name: ImportPolicyNotFound (232) Type: configurationAlarm Package: l3fwd.ImportPolicyNotFound Raised on class: l3fwd.ServiceSiteImportPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: importPolicyDoesNotExist	Release: • N/A
Description: The alarm is raised when a VRF import policy for a VPRN cannot be found. The alarm information includes the policy ID. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has occurred which must be corrected. The VRP import policy must be created and distributed to the NE reporting the problem. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-322 InBandManagementConnectionDown

Alarm	Attributes	Applicable major release
Name: InBandManagementConnectionDown (139) Type: communicationsAlarm Package: netw.InBandManagementConnectionDown Raised on class: netw.NodeDiscoveryControl	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: managementConnectionDown	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function over an in-band connection.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM		

Table 39-323 IncompatibleCapacity

Alarm	Attributes	Applicable major release
Name: IncompatibleCapacity (1166) Type: communicationsAlarm Package: equipment.IncompatibleCapacity Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompatibleCapacity	Release: • N/A

Table 39-323 IncompatibleCapacity (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when there is a radio capacity incompatibility.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-324 IncompatibleFrequency (mwa)

Alarm	Attributes	Applicable major release
Name: IncompatibleFrequency (683) Type: communicationsAlarm Package: mwa.IncompatibleFrequency Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompatibleFrequency	Release: • N/A
Description: The alarm is raised when a provisioned MPT frequency is incompatible with the MPT hardware.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-325 IncompatibleModulationParam (mwa)

Alarm	Attributes	Applicable major release
Name: IncompatibleModulationParam (1144) Type: communicationsAlarm Package: mwa.IncompatibleModulationParam Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompatibleModulationParam	Release: • N/A
Description: The alarm is raised when the provisioned modulation parameters are incompatible with the MPT hardware.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-326 IncompatibleProtection (mwa)

Alarm	Attributes	Applicable major release
Name: IncompatibleProtection (4824) Type: communicationsAlarm Package: mwa.IncompatibleProtection Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompatibleProtection	Release: • N/A
Description: The alarm is raised when a incompatible protection scheme is selected.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-327 IncompatibleShifter (mwa)

Alarm	Attributes	Applicable major release
Name: IncompatibleShifter (685) Type: communicationsAlarm Package: mwa.IncompatibleShifter Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Incompatibleshifter	Release: • N/A
Description: The alarm is raised when the provisioned MPT shifter parameters are incompatible with the MPT hardware.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-328 IncompatibleTxPower

Alarm	Attributes	Applicable major release
Name: IncompatibleTxPower (4825) Type: communicationsAlarm Package: mwa.IncompatibleTxPower Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncompatibleTxPower	Release: • N/A
Description: The alarm is raised when the provisioned MPT transmit power is incompatible with the MPT hardware.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-329 IncompleteConfig (lag)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: lag.IncompleteConfig Raised on class: lag.MultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when an MC LAG has fewer than two members.		
Raising condition: ('numberOfMembers' NOT EQUAL '2')		
Clearing condition: ('numberOfMembers' EQUAL '2')		
Remedial action: Configure the missing peered object.		

Table 39-330 IncompleteConfig (rmon)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: rmon.IncompleteConfig Raised on classes: • rmon.Alarm • rmon.Event	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when an object is created with default values but not yet made active.		
Raising condition: ('Status' EQUAL 'Under Creation')		
Clearing condition: ('Status' NOT EQUAL 'Under Creation')		
Remedial action: The object is created with default values but not yet made active. Please activate.		

Table 39-331 IncompleteConfig (bundle)

Alarm	Attributes	Applicable major release
Name: IncompleteConfig (294) Type: configurationAlarm Package: bundle.IncompleteConfig Raised on class: bundle.MultiChassisApsInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when there are not exactly two APS bundles in an APS group.		
Raising condition: (('Number of members' NOT EQUAL '2'))		
Clearing condition: (('Number of members' EQUAL '2'))		
Remedial action: Configure the missing peered object.		

Table 39-332 InconsistenciesOnNode

Alarm	Attributes	Applicable major release
Name: InconsistenciesOnNode (1077) Type: integrityViolation Package: netw.InconsistenciesOnNode Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inconsistenciesOnNode	Release: • N/A
Description: The alarm is raised when a device detects one or more configuration inconsistencies. On a 9500 MPR, this can be caused by cross-connect creation failure during service creation.		
Remedial action: Please click on the clear inconsistencies button from the NE properties GUI form to clear the inconsistencies.		

Table 39-333 InstallDirectoryDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: InstallDirectoryDiskSpaceBelowThreshold (612) Type: databaseAlarm Package: db.InstallDirectoryDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary or standalone database installation disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The Oracle Proxy purges the log based on database file policy configuration. Reducing the number of archives to keep and/or size of the log files or increasing the available disk space will resolve the problem. If alarm persists please contact your Nokia support representative for assistance.		

Table 39-334 InstanceIdMismatch

Alarm	Attributes	Applicable major release
Name: InstanceIdMismatch (416) Type: configurationAlarm Package: srrp.InstanceIdMismatch Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: instanceIdMismatch	Release: • N/A
Description: The alarm is raised when a local SRRP SAP is backed up by a different SRRP instance on a remote peer.		
Remedial action: Reconfigure the instance so that the peer SRRP instances have the same ID.		

Table 39-335 InterCompoundLinkDown

Alarm	Attributes	Applicable major release
Name: InterCompoundLinkDown (9015) Type: communicationsAlarm Package: optical.InterCompoundLinkDown Raised on class: optical.OpticalLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when any end point of the inter-compound Optical Link is operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the Link End points to understand why the underlying transport network is unreliable.		

Table 39-336 InterfaceDbDescriptAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceDbDescriptAuthFailure (46) Type: authenticationAlarm Package: ospf.InterfaceDbDescriptAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a dbDescript packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-337 InterfaceDbDescriptConfig

Alarm	Attributes	Applicable major release
Name: InterfaceDbDescriptConfig (40) Type: configurationAlarm Package: ospf.InterfaceDbDescriptConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives a dbDescript packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		

Table 39-337 InterfaceDbDescriptConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-338 InterfaceHelloAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceHelloAuthFailure (45) Type: authenticationAlarm Package: ospf.InterfaceHelloAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-339 InterfaceHelloConfig

Alarm	Attributes	Applicable major release
Name: InterfaceHelloConfig (39) Type: configurationAlarm Package: ospf.InterfaceHelloConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-340 InterfaceLsAckAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceLsAckAuthFailure (49) Type: authenticationAlarm Package: ospf.InterfaceLsAckAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		

Table 39-340 InterfaceLsAckAuthFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-341 InterfaceLsAckConfig

Alarm	Attributes	Applicable major release
Name: InterfaceLsAckConfig (43) Type: configurationAlarm Package: ospf.InterfaceLsAckConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-342 InterfaceLsReqAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceLsReqAuthFailure (47) Type: authenticationAlarm Package: ospf.InterfaceLsReqAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-343 InterfaceLsReqConfig

Alarm	Attributes	Applicable major release
Name: InterfaceLsReqConfig (41) Type: configurationAlarm Package: ospf.InterfaceLsReqConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		

Table 39-343 InterfaceLsReqConfig (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-344 InterfaceLsUpdateAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceLsUpdateAuthFailure (48) Type: authenticationAlarm Package: ospf.InterfaceLsUpdateAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsUpdate packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-345 InterfaceLsUpdateConfig

Alarm	Attributes	Applicable major release
Name: InterfaceLsUpdateConfig (42) Type: configurationAlarm Package: ospf.InterfaceLsUpdateConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives an lsUpdate packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-346 InterfaceNullPacketAuthFailure

Alarm	Attributes	Applicable major release
Name: InterfaceNullPacketAuthFailure (50) Type: authenticationAlarm Package: ospf.InterfaceNullPacketAuthFailure Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a non-virtual interface from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		

Table 39-346 InterfaceNullPacketAuthFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The alarm signifies that a null packet has been received on a non-virtual interface from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-347 InterfaceNullPacketConfig

Alarm	Attributes	Applicable major release
Name: InterfaceNullPacketConfig (44) Type: configurationAlarm Package: ospf.InterfaceNullPacketConfig Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifTypeMismatch • nullRouterId • ifAdminDown • ifPassive • subnetMismatch	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a non-virtual interface from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a null packet has been received on a non-virtual interface from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-348 InterfaceRxBadPacket

Alarm	Attributes	Applicable major release
Name: InterfaceRxBadPacket (51) Type: communicationsAlarm Package: ospf.InterfaceRxBadPacket Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hello Applicable probable causes: • hello • dbDescript • lsReq • lsUpdate • lsAck • nullPacket	Release: • N/A
Description: The alarm is raised when an NE cannot parse an OSPF packet that it receives on a non-virtual interface.		
Remedial action: Informational - an NE cannot parse an OSPF packet that it receives on a non-virtual interface.		

Table 39-349 InternalLinkDown

Alarm	Attributes	Applicable major release
Name: InternalLinkDown (9016) Type: communicationsAlarm Package: optical.InternalLinkDown Raised on class: optical.OpticalLink	Severity: cleared Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when any end point of the internal Optical Link is operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the Link End points to understand why the underlying transport network is unreliable.		

Table 39-350 InterRedundantMPTCommunicationFailure

Alarm	Attributes	Applicable major release
Name: InterRedundantMPTCommunicationFailure (4826) Type: communicationsAlarm Package: mwa.InterRedundantMPTCommunicationFailure Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InternalCommunicationProblem	Release: • N/A
Description: The alarm is raised when a MPT detects a Inter Redundant MPTs Communication Failure		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-351 InterXPolarizedMPTCommunicationFailure

Alarm	Attributes	Applicable major release
Name: InterXPolarizedMPTCommunicationFailure (4827) Type: communicationsAlarm Package: mwa.InterXPolarizedMPTCommunicationFailure Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: InternalCommunicationProblem	Release: • N/A
Description: The alarm is raised when a MPT detects a Inter X-Polarized MPTs Communication Failure		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-352 InvalidBOFAddress

Alarm	Attributes	Applicable major release
Name: InvalidBOFAddress (1141) Type: communicationsAlarm Package: netw.InvalidBOFAddress Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: invalidBOF	Release: • N/A
Description: The alarm is raised during a network topology rescan in which the 5620 SAM does not find a previously configured NE BOF address, and the Management IP Selection of the NE is set to one of the following: - Out Of Band Preferred - In Band Preferred		
Remedial action: A configuration error has been made which must be corrected. The BOF address must be configured on the NE.		

Table 39-353 invalidHDMVersion

Alarm	Attributes	Applicable major release
Name: invalidHDMVersion (12418) Type: equipmentAlarm Package: femto.invalidHDMVersion Raised on class: femto.HDMCluster	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidHDMVersion	Release: • N/A
Description: Invalid HDM Version 4.1.x		
Remedial action: HDM Version 4.1.x is not supported. Configure HDM 5.0.3 or later version.		

Table 39-354 InvalidJoinPrune

Alarm	Attributes	Applicable major release
Name: InvalidJoinPrune (185) Type: communicationsAlarm Package: pim.InvalidJoinPrune Raised on class: pim.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidJoinPruneReceived	Release: • N/A

Table 39-354 InvalidJoinPrune (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the RP address in a Join Prune message is not the RP for the group specified in the message.		
Remedial action: Informational - please make sure the RP address in a Join Prune message is the RP for the group specified		

Table 39-355 InvalidRegister

Alarm	Attributes	Applicable major release
Name: InvalidRegister (186) Type: communicationsAlarm Package: pim.InvalidRegister Raised on class: pim.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidJoinRegisterReceived	Release: • N/A
Description: The alarm is raised when the RP address in a Register message is not the RP for the group specified in the message.		
Remedial action: Informational - please make sure the RP address in a Register message is the RP for the group specified		

Table 39-356 invalidRPLoopbackInterfaceConfig

Alarm	Attributes	Applicable major release
Name: invalidRPLoopbackInterfaceConfig (269) Type: configurationAlarm Package: pim.invalidRPLoopbackInterfaceConfig Raised on class: pim.VirtualAnyCastRP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidRPLoopbackIfConfig	Release: • N/A
Description: The alarm is raised when an RP loopback interface configuration is invalid.		
Remedial action: A configuration error has occurred that must be corrected. Please check the global Virtual Anycast RP configuration and its operational status flag so that the loopback is properly configured, PIM is enabled on the loopback interface.		

Table 39-357 IOReadFileFromDisk

Alarm	Attributes	Applicable major release
Name: IOReadFileFromDisk (5136) Type: serverAlarm Package: server.IOReadFileFromDisk Raised on class: server.SamServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskProblem	Release: • N/A
Description: The alarm is raised when SAM cannot read a file from disk.		
Remedial action: Check the additional text of the alarm for more details. Possible causes are insufficient file permissions, disk corruption or general disk hardware failure. The additional text will provide guidance as to the specifics of the problem.		

Table 39-358 IOWriteFileToDisk

Alarm	Attributes	Applicable major release
Name: IOWriteFileToDisk (5137) Type: serverAlarm Package: server.IOWriteFileToDisk Raised on class: server.SamServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskProblem	Release: • N/A
Description: The alarm is raised when SAM cannot write a file to disk.		
Remedial action: Check the additional text of the alarm for more details. Possible causes are lack of disk space, insufficient file permissions, disk corruption or or general disk hardware failure. The additional text will provide guidance as to the specifics of the problem.		

Table 39-359 IpAddressManaged

Alarm	Attributes	Applicable major release
Name: IpAddressManaged (4388) Type: IpAddressManaged Package: ptp.IpAddressManaged Raised on class: ptp.SourceEntryPoint	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IpAddressManaged	Release: • N/A
Description: The alarm is raised when unmanaged IP address becomes managed virtual router IP address.		
Remedial action: The source entry point unmanaged IP address becomes managed virtual router IP address. Please re-configure source entry point.		

Table 39-360 IpAddressOverlap

Alarm	Attributes	Applicable major release
Name: IpAddressOverlap (3318) Type: configurationAlarm Package: rtr.IpAddressOverlap Raised on class: rtr.VirtualRouterIpAddress	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IpAddressOverlap	Release: • N/A
Description: The alarm is raised when the IP addresses configured on different VPRN sites within service overlap.		
Remedial action: Please check the IP Addresses configured on different VPRN sites have no overlap.		

Table 39-361 IPListMismatch

Alarm	Attributes	Applicable major release
Name: IPListMismatch (282) Type: configurationAlarm Package: vrrp.IPListMismatch Raised on class: vrrp.AbstractInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nonMatchingBackupAddress-List	Release: • N/A

Table 39-361 IPListMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the IP address list in an advertisement message from the current master does not match the configured IP address list.		
Remedial action: Check the configured IP addresses, make sure they match the advertised IP addresses from the master VRRP instance.		

Table 39-362 IpPathDown

Alarm	Attributes	Applicable major release
Name: IpPathDown (1916) Type: topologyAlarm Package: monpath.IpPathDown Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipPathDown	Release: • N/A
Description: This alarm is raised when the re-calculation by the CPAA shows that no IP Path is available.		
Remedial action: Informational - The IP path record provides an Error code which provides a clue on why the path is down.		

Table 39-363 IpPathMonitorFailedRetryThresholdCrossed

Alarm	Attributes	Applicable major release
Name: IpPathMonitorFailedRetryThresholdCrossed (400) Type: topologyAlarm Package: monpath.IpPathMonitorFailedRetryThresholdCrossed Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipPathCouldNotBeDetermined	Release: • N/A
Description: The alarm is raised when the 5650 CPAM cannot set up an IP path monitor after the number of attempts specified by the cpamManagedRoute problematicThresholdAlarmAfter value in the nms-server.xml file. The alarm is raised if the cpamManagedRoute problematicRetryStrategy value in nms-server.xml is set to countdown. The default problematicRetryStrategy value of reactive prevents the alarm from being raised.		
Remedial action: Informational - The Retry strategy can be modified in nms-server.xml. This alarm is not raised for the default retry strategy, reactive.		

Table 39-364 IpPathMonitorRetryAttemptsExhausted

Alarm	Attributes	Applicable major release
Name: IpPathMonitorRetryAttemptsExhausted (401) Type: topologyAlarm Package: monpath.IpPathMonitorRetryAttemptsExhausted Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ipPathCouldNotBeDetermined	Release: • N/A

Table 39-364 IpPathMonitorRetryAttemptsExhausted (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5650 CPAM stops trying to set up an IP path monitor after the number of attempts specified by the cpamManagedRoute problematicDeadAfter value in the nms-server.xml file. The alarm is raised if the cpamManagedRoute problematicRetryStrategy value in nms-server.xml is set to countdown. The default problematicRetryStrategy value of reactive prevents the alarm from being raised.		
Remedial action: Informational - The Retry strategy can be modified in nms-server.xml. This alarm is not raised for the default retry strategy, reactive.		

Table 39-365 IpPathMulticastWarning

Alarm	Attributes	Applicable major release
Name: IpPathMulticastWarning (1917) Type: topologyAlarm Package: monpath.IpPathMulticastWarning Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IpPathSegmentNotMulticas-tEnabled	Release: • N/A
Description: If IP Path is enabled for monitoring Multicast, the alarm is raised when at least one IP Path segment is not Multicast enabled. The alarm is cleared when all the segments are Multicast enabled.		
Remedial action: Informational - The segments without PIM interface enabled can be obtained from path record. PIM should be enabled on these interfaces in order for alarm to be cleared.		

Table 39-366 IPsecInterfaceBfdSessionDown

Alarm	Attributes	Applicable major release
Name: IPsecInterfaceBfdSessionDown (3324) Type: bfdSessionAlarm Package: service.IPsecInterfaceBfdSessionDown Raised on class: service.IPsecInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionDown	Release: • N/A
Description: The alarm is raised when a BFD session is operationally down.		
Remedial action: This alarm is raised when a BFD session on an IPsec interface goes down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-367 IPsecInterfaceBfdSessionFlapped

Alarm	Attributes	Applicable major release
Name: IPsecInterfaceBfdSessionFlapped (3905) Type: bfdSessionAlarm Package: service.IPsecInterfaceBfdSessionFlapped Raised on class: service.IPsecInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionFlapped	Release: • N/A
Description: The alarm is raised when a BFD session transitions from Up to Down and back to Up within the BFD operational state transition interval.		
Remedial action: The BFD session on an IPsec interface has transitioned from Up to Down and back to Up within the configured BFD Flapping Interval.		

Table 39-368 IPsecInterfaceBfdSessionMissing

Alarm	Attributes	Applicable major release
Name: IPsecInterfaceBfdSessionMissing (3325) Type: bfdSessionAlarm Package: service.IPsecInterfaceBfdSessionMissing Raised on class: service.IPsecInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bfdSessionMissing	Release: • N/A
Description: The alarm is raised when a previously present BFD session is absent.		
Remedial action: This alarm is raised when a previously present BFD session on an IPsec interface is absent. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the near end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 39-369 IPSecRUSAFailToAddRoute

Alarm	Attributes	Applicable major release
Name: IPSecRUSAFailToAddRoute (5185) Type: processingErrorAlarm Package: ipsec.IPSecRUSAFailToAddRoute Raised on class: ipsec.IPSecSecuredVpnManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IPSecRUSAFailToAddRoute	Release: • N/A
Description: The trap tIPsecRUSAFailToAddRoute is sent when adding route to tIPsecRUSARemAddr for the remote-user tunnel fails with reason indicated by tIPsecNotifReason.		
Remedial action: Informational - Please see reason for failure.		

Table 39-370 IPsecRUTnlFailToCreate

Alarm	Attributes	Applicable major release
Name: IPsecRUTnlFailToCreate (5186) Type: processingErrorAlarm Package: ipsec.IPsecRUTnlFailToCreate Raised on class: ipsec.IPSecGateway	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IPsecRUTnlFailToCreate	Release: • N/A
Description: This alarm is sent when creation of a remote-user tunnel fails with reason indicated by notifReason.		
Remedial action: Informational - Please see reason for failure.		

Table 39-371 IPsecRUTnlRemoved

Alarm	Attributes	Applicable major release
Name: IPsecRUTnlRemoved (9611) Type: processingErrorAlarm Package: ipsec.IPsecRUTnlRemoved Raised on class: ipsec.IPSecGateway	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IPsecRUTnlRemoved	Release: • N/A
Description: This alarm is sent when creation of a remote-user tunnel is removed under certain reasons, which are indicated by notifReason (e.g., failed to renew private address lease with DHCP server)		
Remedial action: Informational - Please see reason for failure.		

Table 39-372 IsaAaGrpBitRate

Alarm	Attributes	Applicable major release
Name: IsaAaGrpBitRate (2948) Type: equipmentAlarm Package: isa.IsaAaGrpBitRate Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpBitRate	Release: • N/A
Description: The alarm is raised when the current bit rate on the MDA in the ISA-AA group is greater than or equal to tmnxBsxBitRate-HighWatermark, and the prior bit rate is less than the threshold.		
Remedial action: The current bit rate on the MDA in the ISA-AA group is greater than or equal to the configured Bit Rate High Watermark. The threshold configured should be revisited to ensure that it is not set too low. To disable the notification, set the Packet Rate High Watermark to maximum.		

Table 39-373 IsaAaGrpCapCostThres

Alarm	Attributes	Applicable major release
Name: IsaAaGrpCapCostThres (835) Type: equipmentAlarm Package: isa.IsaAaGrpCapCostThres Raised on class: isa.AaGroupMember	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: IsaAaGrpCapCostThres	Release: • N/A

Table 39-373 IsaAaGrpCapCostThres (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the capacity cost for an MDA in an ISA-AA group reaches the configured threshold.		
Remedial action: The capacity cost high threshold for the MDA in the ISA-AA group has been reached.		

Table 39-374 IsaAaGrpFailure

Alarm	Attributes	Applicable major release
Name: IsaAaGrpFailure (564) Type: equipmentAlarm Package: isa.IsaAaGrpFailure Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: isaAaGrpFailure	Release: • N/A
Description: The alarm is raised when an ISA-AA Group has no configured primary MDA or the number of active MDAs is not equal to the number of configured primary MDAs.		
Remedial action: There is a failure on the ISA-AA group. Ensure that ISA-AA group has a primary MDA group member configured, and that the number of active MDAs is equal to the number of configured primary MDAs.		

Table 39-375 IsaAaGrpFlowFull

Alarm	Attributes	Applicable major release
Name: IsaAaGrpFlowFull (566) Type: equipmentAlarm Package: isa.IsaAaGrpFlowFull Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpFlowFull	Release: • N/A
Description: The alarm is raised when an ISA-AA group uses a greater number of flow records than the value specified by tmnxBsxFlowFullHighWatermark.		
Remedial action: The number of flow records that the ISA-AA group is using is greater than or equal to the configured Flow Full High Watermark. The threshold configured should be revisited to ensure that it is not set too low.		

Table 39-376 IsaAaGrpFlowSetup

Alarm	Attributes	Applicable major release
Name: IsaAaGrpFlowSetup (2949) Type: equipmentAlarm Package: isa.IsaAaGrpFlowSetup Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpFlowSetup	Release: • N/A
Description: The alarm is raised when the current flow setup rate on the MDA in the ISA-AA group is greater than or equal to tmnxBsxFlowSetupHighWatermark, and the prior bit rate is less than the threshold.		

Table 39-376 IsaAaGrpFlowSetup (continued)

Alarm	Attributes	Applicable major release
Remedial action: The current flow setup rate on the MDA in the ISA-AA group is greater than or equal to the configured Flow Setup High Watermark. The threshold configured should be revisited to ensure that it is not set too low. To disable the notification, set the Flow Setup High Watermark to maximum.		

Table 39-377 IsaAaGrpFmSbWaSBufOvld

Alarm	Attributes	Applicable major release
Name: IsaAaGrpFmSbWaSBufOvld (2950) Type: equipmentAlarm Package: isa.IsaAaGrpFmSbWaSBufOvld Raised on class: isa.AaGroupMember	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpFmSbWaSBufOvld	Release: • N/A
Description: The alarm is raised when the current weighted average shared buffer for an ISA in the from subscriber direction is greater than or equal to a high water mark in a normal, non-overloaded, state.		
Remedial action: The ISA-AA Egress From-Subscriber buffer pool has entered an overload state as determined by the configured Buffer Utilization High Watermark. The threshold configured should be revisited to ensure it is not set too low. To disable the notification, set the Buffer Utilization High Watermark to the maximum.		

Table 39-378 IsaAaGrpNonRedundant

Alarm	Attributes	Applicable major release
Name: IsaAaGrpNonRedundant (565) Type: equipmentAlarm Package: isa.IsaAaGrpNonRedundant Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpNonRedundant	Release: • N/A
Description: The alarm is raised when an ISA-AA Group has a configured backup MDA but there is no standby MDA available.		
Remedial action: The ISA-AA Group has a configured backup MDA but there is no standby MDA available. Check that the configured standby MDA is active and operationally up. There may be a fault with the ISA Application Assurance MDA.		

Table 39-379 IsaAaGrpOvrldCutthru

Alarm	Attributes	Applicable major release
Name: IsaAaGrpOvrldCutthru (2951) Type: equipmentAlarm Package: isa.IsaAaGrpOvrldCutthru Raised on class: isa.AaGroupMember	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpOvrldCutthru	Release: • N/A
Description: The alarm is raised when cut through processing starts on an ISA MDA.		
Remedial action: Overload Cut-Through is enabled on the ISA-AA Group. All traffic is cut-through and the ISA-AA MDA is overloaded. Disable Overload Cut-Through if this is not required.		

Table 39-380 IsaAaGrpPacketRate

Alarm	Attributes	Applicable major release
Name: IsaAaGrpPacketRate (2952) Type: equipmentAlarm Package: isa.IsaAaGrpPacketRate Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpPacketRate	Release: • N/A
Description: The alarm is raised when the current packet rate on the MDA in the ISA-AA group is greater than or equal to tmnxBsxPacketRateHighWatermark, and the prior rate is less than this threshold.		
Remedial action: The current packet rate on the MDA in the ISA-AA group is greater than or equal to the configured Packet Rate High Watermark. The threshold configured should be revisited to ensure that it is not set too low. To disable the notification, set the Packet Rate High Watermark to maximum.		

Table 39-381 IsaAaGrpSwitchover

Alarm	Attributes	Applicable major release
Name: IsaAaGrpSwitchover (567) Type: equipmentAlarm Package: isa.IsaAaGrpSwitchover Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaAaGrpSwitchover	Release: • N/A
Description: The alarm is raised when an ISA-AA group experiences an activity switch from one ISA-AA to another.		
Remedial action: The ISA-AA Group has performed an activity switch from one ISA-AA MDA to another.		

Table 39-382 IsaAaGrpToSbWaSBufOvld

Alarm	Attributes	Applicable major release
Name: IsaAaGrpToSbWaSBufOvld (2953) Type: equipmentAlarm Package: isa.IsaAaGrpToSbWaSBufOvld Raised on class: isa.AaGroupMember	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IsaAaGrpToSbWaSBufOvld	Release: • N/A
Description: The alarm is raised when the current weighted average shared buffer use for an ISA in the To subscriber direction, is greater than or equal to a high water mark, after being in a normal or non-overloaded state.		
Remedial action: The ISA-AA Egress To-Subscriber buffer pool has entered an overload state as determined by the configured Buffer Utilization High Watermark. The threshold configured should be revisited to ensure it is not set too low. To disable the notification, set the Buffer Utilization High Watermark to the maximum.		

Table 39-383 IsaDatapathCpuUsage

Alarm	Attributes	Applicable major release
Name: IsaDatapathCpuUsage (11174) Type: equipmentAlarm Package: isa.IsaDatapathCpuUsage Raised on class: isa.AaGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isaDatapathCpuUsage	Release: • N/A
Description: The alarm is raised when the current datapath CPU usage on the MDA in the ISA-AA group is greater than or equal to the tmnxBsxDatapathCpuHighWatermark and the prior usage was less than this threshold.		
Remedial action: The current datapath CPU usage on the MDA in the ISA-AA group is greater than or equal to the configured Datapath CPU Usage High Watermark. The threshold configured should be revisited to ensure that it is not set too low. To disable the notification, set the Datapath CPU Usage High Watermark to maximum.		

Table 39-384 IsidMisconfiguration (vpls)

Alarm	Attributes	Applicable major release
Name: IsidMisconfiguration (592) Type: configurationAlarm Package: vpls.IsidMisconfiguration Raised on class: vpls.AbstractVpls	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: isidInconsistent	Release: • N/A
Description: The alarm is raised when service sites use inconsistent I-SID values for a PBB backbone. The alarm is raised against a VPLS or M-VPLS service.		
Raising condition: ('operationalFlags'anyBit'ISID Inconsistent')		
Clearing condition: NOT (('operationalFlags'anyBit'ISID Inconsistent'))		
Remedial action: All service sites must use consistent I-SID values for a PBB backbone.		

Table 39-385 IsidMisconfiguration (epipe)

Alarm	Attributes	Applicable major release
Name: IsidMisconfiguration (592) Type: configurationAlarm Package: epipe.IsidMisconfiguration Raised on class: epipe.Epipe	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: isidInconsistent	Release: • N/A
Description: The alarm is raised when Epipe service sites that are bound to a PBB backbone use different ISID values.		
Raising condition: ('operationalFlags'anyBit'ISID Inconsistent')		
Clearing condition: NOT (('operationalFlags'anyBit'ISID Inconsistent'))		
Remedial action: All service sites must use consistent I-SID values for a PBB backbone.		

Table 39-386 IsisAreaMismatch

Alarm	Attributes	Applicable major release
Name: IsisAreaMismatch (156) Type: configurationAlarm Package: isis.IsisAreaMismatch Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • N/A
Description: The alarm is raised when IS-IS receives a Hello PDU from an IS with which it does not share an area address.		
Remedial action: Check whether NET address is configured and the AREA ID between two adjacencies are not the same.		

Table 39-387 IsisAuthFailure

Alarm	Attributes	Applicable major release
Name: IsisAuthFailure (155) Type: authenticationAlarm Package: isis.IsisAuthFailure Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authFailure	Release: • N/A
Description: The alarm is raised when IS-IS receives a PDU that contains incorrect authentication information.		
Remedial action: The authentication information on the ISIS Site needs to be changed to match its neighbours.		

Table 39-388 IsisAuthTypeFailure

Alarm	Attributes	Applicable major release
Name: IsisAuthTypeFailure (154) Type: authenticationAlarm Package: isis.IsisAuthTypeFailure Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: authFailure	Release: • N/A
Description: The alarm is raised when IS-IS receives a PDU that contains the wrong authentication type.		
Remedial action: The authentication information on the ISIS Site needs to be changed to match its neighbours.		

Table 39-389 IsisExportLimitDropped

Alarm	Attributes	Applicable major release
Name: IsisExportLimitDropped (838) Type: configurationAlarm Package: isis.IsisExportLimitDropped Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitDropped	Release: • N/A
Description: The alarm is raised when the number of routes exported from the route table to an IS-IS level drops below the Export Limit value for the level.		
Remedial action: Informational.		

Table 39-390 IsisExportLimitReached

Alarm	Attributes	Applicable major release
Name: IsisExportLimitReached (839) Type: configurationAlarm Package: isis.IsisExportLimitReached Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitReached	Release: • N/A
Description: The alarm is raised when the number of routes exported from the route table to an IS-IS level is equal to the Export Limit value for the level.		
Remedial action: Informational - the number of routes exported from the route table to an IS-IS level is equal to the Export Limit value for the level		

Table 39-391 IsisExportLimitWarning

Alarm	Attributes	Applicable major release
Name: IsisExportLimitWarning (840) Type: configurationAlarm Package: isis.IsisExportLimitWarning Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitWarning	Release: • N/A
Description: The alarm is raised when the number of routes exported from the route table to an IS-IS level is equal to the Export Limit percentage specified by the Export Limit Log Percent value.		
Remedial action: Informational - the number of routes exported from the route table to an IS-IS level is equal to the Export Limit percentage specified by the Export Limit Log Percent value.		

Table 39-392 IsisLspRateThresholdExceeded

Alarm	Attributes	Applicable major release
Name: IsisLspRateThresholdExceeded (376) Type: topologyAlarm Package: topology.IsisLspRateThresholdExceeded Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableIGPNetwork	Release: • N/A
Description: The alarm is raised when the IS-IS LSP rate exceeds the maximum allowed value because of an unstable IGP network.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-393 IsisLspThresholdExceeded

Alarm	Attributes	Applicable major release
Name: IsisLspThresholdExceeded (375) Type: topologyAlarm Package: topology.IsisLspThresholdExceeded Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: largeIGPNetwork	Release: • N/A

Table 39-393 IsisLspThresholdExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of IS-IS LSPs exceeds the maximum allowed value because of a large IGP network.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-394 IsisManualAddressDrops

Alarm	Attributes	Applicable major release
Name: IsisManualAddressDrops (157) Type: configurationAlarm Package: isis.IsisManualAddressDrops Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: noError	Release: • N/A
Description: The alarm is raised when a manual area address assigned to an IS is ignored during a route computation.		
Remedial action: Informational - no corrective action required.		

Table 39-395 IsisPrefixLimitWarning

Alarm	Attributes	Applicable major release
Name: IsisPrefixLimitWarning (9647) Type: configurationAlarm Package: isis.IsisPrefixLimitWarning Raised on class: isis.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: prefixLimitWarning	Release: • N/A
Description: The alarm is raised when number of prefixes in the system reaches the PrefixLimitThreshold or the PrefixLimit		
Remedial action: Increase the IS-IS prefix limit for this instance.		

Table 39-396 IsisReachabilityThresholdExceeded

Alarm	Attributes	Applicable major release
Name: IsisReachabilityThresholdExceeded (377) Type: topologyAlarm Package: topology.IsisReachabilityThresholdExceeded Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: manyExternalLSAsFloodingIn-toIGP	Release: • N/A
Description: The alarm is raised when the IS-IS reachability value exceeds the maximum allowed value because too many external LSAs are flooding the IGP.		
Remedial action: User configured alarm for monitoring purpose. The advertised routes can be viewed using CPAM IGP prefix list.		

Table 39-397 IsisRejectedAdjacency

Alarm	Attributes	Applicable major release
Name: IsisRejectedAdjacency (214) Type: adjacencyAlarm Package: isis.IsisRejectedAdjacency Raised on class: isis.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives a vRtrIsisRejectedAdjacency trap, which indicates that an adjacency cannot be established in response to a Hello PDU from an IS because of a lack of resources.		
Remedial action: Informational, might have exceeded the maximum number of adjacencies allowed.		

Table 39-398 IsisRejectedAdjacencySID

Alarm	Attributes	Applicable major release
Name: IsisRejectedAdjacencySID (9054) Type: configurationAlarm Package: isis.IsisRejectedAdjacencySID Raised on class: isis.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isisRejectedAdjacencySID	Release: • N/A
Description: The notification is sent when node do not establish an adjacency SID due to a lack of resources.		
Remedial action: Informational, When an operationally up interface is deleted, the ADJ-SID can be reused by any interface which is waiting to receive an ADJ-SID.		

Table 39-399 IsisSIDError

Alarm	Attributes	Applicable major release
Name: IsisSIDError (9055) Type: configurationAlarm Package: isis.IsisSIDError Raised on class: isis.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isisSIDError	Release: • N/A
Description: This notification is generated when ISIS receives an IOM or CPM failure (system exhausted ILM, NHLFE, duplicate SID) while resolving and programming a received prefix SID.		
Remedial action: In case of system exhaustion, the IGP instance goes into overload. The operator must manually clear the IGP overload condition after freeing resources. IGP will attempt to program at the next SPF all tunnels which previously failed the programming operation		

Table 39-400 IsisSIDNotInLabelRange

Alarm	Attributes	Applicable major release
Name: IsisSIDNotInLabelRange (9056) Type: configurationAlarm Package: isis.IsisSIDNotInLabelRange Raised on class: isis.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: isisSIDNotInLabelRange	Release: • N/A
Description: This notification is generated when ISIS receives a SID which is not within the label range of the next hop router		
Remedial action: The SID range needs to be change to include adjacent SID received.		

Table 39-401 JMSClientMessagesRemoved

Alarm	Attributes	Applicable major release
Name: JMSClientMessagesRemoved (532) Type: communicationsAlarm Package: security.JMSClientMessagesRemoved Raised on class: security.User	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: maximumExceededMessages	Release: • N/A
Description: The alarm is raised when the number of JMS messages that are queued for a 5620 SAM client exceeds the allowed number. The 5620 SAM subsequently deletes messages to keep the number within the allowed range.		
Remedial action: Information - if the alarm persists or is occurring frequently then investigation is required to determine a) why the underlying transport network is unreliable or b) why the OSS client which initiated the JMS connection is unable to process the JMS messages.		

Table 39-402 JMSDurableClientReset

Alarm	Attributes	Applicable major release
Name: JMSDurableClientReset (530) Type: communicationsAlarm Package: security.JMSDurableClientReset Raised on class: security.User	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: jmsServerRestart	Release: • N/A
Description: The alarm is raised when a durable JMS client is removed from the 5620 SAM because of a JMS server restart or switchover.		
Remedial action: Informational - the JMS server has restarted. If the alarm persists contact your Nokia support representative for assistance.		

Table 39-403 JMSDurableClientUnsubscribed

Alarm	Attributes	Applicable major release
Name: JMSDurableClientUnsubscribed (531) Type: communicationsAlarm Package: security.JMSDurableClientUnsubscribed Raised on class: security.User	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: maximumExceededMessages	Release: • N/A
Description: The alarm is raised when a durable JMS client is unsubscribed and removed from the 5620 SAM.		
Remedial action: Informational - the durable message limit for the topic has been reached and disconnected clients are automatically unsubscribed. An investigation is required to understand a) why the underlying transport network is unreliable or b) why the OSS client which initiated the JMS connection is unable to process the JMS messages.		

Table 39-404 JMSServerDown

Alarm	Attributes	Applicable major release
Name: JMSServerDown (360) Type: communicationsAlarm Package: netw.JMSServerDown Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when JMS communication fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the SAM server and the OSS system is unreliable.		

Table 39-405 JMSServerMemoryLow

Alarm	Attributes	Applicable major release
Name: JMSServerMemoryLow (3693) Type: communicationsAlarm Package: security.JMSServerMemoryLow Raised on class: security.User	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: jmsMessageQueueBacklog	Release: • N/A
Description: The alarm is raised when available memory on the JMS server is low.		
Remedial action: This is probably caused by SAM GUI clients or OSS clients having a large backlog of events on the JMS server. If available memory continues to decrease, the client with the largest backlog will be removed by the server. Please see the Additional Text field to identify the client with the largest backlog. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-406 KeyChainAuthFailure

Alarm	Attributes	Applicable major release
Name: KeyChainAuthFailure (421) Type: communicationsAlarm Package: security.KeyChainAuthFailure Raised on class: security.KeyChain	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: keyChainAuthFailure	Release: • N/A
Description: The alarm is raised when an incoming packet is dropped because of a TCP key chain authentication failure.		
Remedial action: A configuration error has been made which must be corrected. The TCP configuration related to authentication differs between the systems upon which the connection endpoints reside. Compare the configuration on the endpoint and correct the mismatch.		

Table 39-407 KPIThresholdCrossingAlarm

Alarm	Attributes	Applicable major release
Name: KPIThresholdCrossingAlarm (11190) Type: qualityOfServiceAlarm Package: sup.KPIThresholdCrossingAlarm Raised on class: sup.SupervisionManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: This alarm is raised on a monitored object when the monitored object has a KPI TCA policy associated with it and the KPI values for KPIs specified in the TCA policy cross the threshold values defined in the TCA policy. KPI TCA Policy is available as a BETA feature for network supervision web application.		
Remedial action: Please see the recomended action specified in the KPI TCA Policy		

Table 39-408 L2tpLnsSePppSessionFailure

Alarm	Attributes	Applicable major release
Name: L2tpLnsSePppSessionFailure (3901) Type: processingErrorAlarm Package: rtr.L2tpLnsSePppSessionFailure Raised on class: rtr.RoutingInstanceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: l2tpLnsSePppSessionFailed	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot create a new L2TP session.		
Remedial action: The alarm is raised when an NE notifies the 5620 SAM that it cannot create a new L2TP session. Verify the configuration to have LNS group assigned to the group tunnel profile or tunnel profile. Additionally, verify the length of the auto-generated subscriber identification.		

Table 39-409 L2tpTunnelBlacklisted

Alarm	Attributes	Applicable major release
Name: L2tpTunnelBlacklisted (4625) Type: processingErrorAlarm Package: l2tp.L2tpTunnelBlacklisted Raised on class: l2tp.TunnelStatus	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tmnxL2tpTunnelBlacklisted	Release: • N/A
Description: This alarm is raised when a L2TP tunnel is added to the tunnel-selection-blacklist. It is automatically cleared when the tunnel is removed from the list.		
Remedial action: In most cases the problem is a configuration mismatch between LAC and LNS, or a problem on LNS. Please refer to the additional text and enable the debug log on event lac-session-setup to figure out the root cause.		

Table 39-410 LacpExpired

Alarm	Attributes	Applicable major release
Name: LacpExpired (3981) Type: equipmentAlarm Package: lag.LacpExpired Raised on class: lag.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LagSubgroupMemberStat-eChange	Release: • N/A
Description: The alarm is raised when Lacp expired on subgroup lag member due to state change.		
Remedial action: The reasons for LACP Expired alarm may vary. The following possible causes of this alarm should be investigated. The partner lag member oper state may have changed or LACP Transmit Standby may have been disabled - this can be remedied by enabling the LACP Transmit Standby on Lag. The partner lag member 802.3ah oper state may have changed - ensure that 802.3ah state is same on both ends. The partner lag member dot1ag state may have changed - ensure that dot1ag state is same on both ends.		

Table 39-411 LagDot1agStateChanged

Alarm	Attributes	Applicable major release
Name: LagDot1agStateChanged (3982) Type: equipmentAlarm Package: lag.LagDot1agStateChanged Raised on class: lag.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Dot1agStateChange	Release: • N/A
Description: The alarm is raised when the subgroup lag member dot1ag state has changed.		
Remedial action: The lag member dot1ag state may have changed - please ensure that dot1ag state is same on both ends.		

Table 39-412 LagEfmOamStateChanged

Alarm	Attributes	Applicable major release
Name: LagEfmOamStateChanged (3983) Type: equipmentAlarm Package: lag.LagEfmOamStateChanged Raised on class: lag.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EfmOamStateChange	Release: • N/A
Description: The alarm is raised when the subgroup lag member efmOam state has changed.		
Remedial action: The lag member 802.3ah oper state may have changed - please ensure that 802.3ah state is same on both ends.		

Table 39-413 LagPartnerOperStateChanged

Alarm	Attributes	Applicable major release
Name: LagPartnerOperStateChanged (3984) Type: equipmentAlarm Package: lag.LagPartnerOperStateChanged Raised on class: lag.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PartnerOperStateChange	Release: • N/A
Description: The alarm is raised when the subgroup lag member partner oper state has changed.		
Remedial action: The lag member oper state may have changed or LACP Transmit Standby may have been disabled - this can be remedied by enabling the LACP Transmit Standby on Lag.		

Table 39-414 LanFailure

Alarm	Attributes	Applicable major release
Name: LanFailure (628) Type: equipmentAlarm Package: equipment.LanFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lanFailure	Release: • N/A
Description: The alarm is raised when a LAN failure is detected.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-415 LastHopIncorrectLabelAction

Alarm	Attributes	Applicable major release
Name: LastHopIncorrectLabelAction (352) Type: configurationAlarm Package: mpls.LastHopIncorrectLabelAction Raised on class: mpls.StaticLsp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LabelActionIsNotPopOnLastHop	Release: • N/A
Description: The alarm is raised when the label action specified for the last hop in a static LSP is not a pop action.		
Remedial action: Ensure the last hop configured with a pop label action, if the last hop node is managed by SAM.		

Table 39-416 LastHopNotMatchingDestination

Alarm	Attributes	Applicable major release
Name: LastHopNotMatchingDestination (351) Type: configurationAlarm Package: mpls.LastHopNotMatchingDestination Raised on class: mpls.StaticLsp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LastHopNotMatchingDestination	Release: • N/A
Description: The alarm is raised when the last hop in a static LSP is not the destination.		
Remedial action: Ensure the last hop configured in the static LSP match the destination of the LSP, if the last hop node is managed by SAM.		

Table 39-417 LatencyMismatchAlarm

Alarm	Attributes	Applicable major release
Name: LatencyMismatchAlarm (8422) Type: integrityViolation Package: gmpls.LatencyMismatchAlarm Raised on class: gmpls.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: latencyMismatch	Release: • N/A
Description: The alarm is raised when the latency configured on the endpoints of the TE Link do not match.		
Remedial action: This alarm indicates that the latency configured on the endpoints of the discovered TE Link do not match. Please make sure the latency values match.		

Table 39-418 LCD

Alarm	Attributes	Applicable major release
Name: LCD (803) Type: communicationsAlarm Package: mpr.LCD Raised on class: mpr.IMALink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfCellDelineation	Release: • N/A

Table 39-418 LCD (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a Loss of Cell Delineation signal is detected on an ASAP MDA.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-419 LdpInterfaceDown

Alarm	Attributes	Applicable major release
Name: LdpInterfaceDown (21) Type: ProtocolAlarm Package: ldp.LdpInterfaceDown Raised on class: ldp.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: protocolDown	Release: • N/A
Description: The alarm is raised when an LDP interface is operationally down.		
Remedial action: Check operational state down reason and state qualifier, then update accordingly.		

Table 39-420 Licensed3RouterLimitExceeded

Alarm	Attributes	Applicable major release
Name: Licensed3RouterLimitExceeded (694) Type: cpamLicensingAlarm Package: security.Licensed3RouterLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 100 percent of the license capacity.		
Raising condition: ('isLicensed3RouterLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensed3RouterLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Third Party Router licenses purchased and available on the CPAM server is insufficient as compared to the number of third party routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-421 Licensed3RouterLimitNearing

Alarm	Attributes	Applicable major release
Name: Licensed3RouterLimitNearing (695) Type: cpamLicensingAlarm Package: security.Licensed3RouterLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 75 to 90 percent of the license capacity.		

Table 39-421 Licensed3RouterLimitNearing (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - The number of Third Party Router licenses purchased and available on the CPAM server is insufficient as compared to the number of third party routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-422 Licensed3RouterLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: Licensed3RouterLimitNearlyExceeded (696) Type: cpamLicensingAlarm Package: security. Licensed3RouterLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of third-party routers in the 5650 CPAM network reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of Third Party Router licenses purchased and available on the CPAM server is insufficient as compared to the number of third party routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-423 LicensedBgpRouteProfileLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedBgpRouteProfileLimitExceeded (5132) Type: cpamLicensingAlarm Package: security. LicensedBgpRouteProfileLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of BGP Route Profiles in the 5650 CPAM reaches 100 percent of the license capacity.		
Raising condition: ('isLicensedBgpProfileLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedBgpProfileLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Bgp Route Profile Module licenses purchased and available on the CPAM server is insufficient as compared to the number of Bgp Route Profiles in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-424 LicensedBgpRouteProfileLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedBgpRouteProfileLimitNearing (5133) Type: cpamLicensingAlarm Package: security.LicensedBgpRouteProfileLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of BGP Route Profiles in the 5650 CPAM reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of Bgp Route Profile Module licenses purchased and available on the CPAM server is insufficient as compared to the number of Bgp Route Profiles in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-425 LicensedBgpRouteProfileLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedBgpRouteProfileLimitNearlyExceeded (5134) Type: cpamLicensingAlarm Package: security.LicensedBgpRouteProfileLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of BGP Route Profiles in the 5650 CPAM reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of Bgp Route Profiles Module licenses purchased and available on the CPAM server is insufficient as compared to the number of BGP Route Profiles in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-426 LicensedBigRouterLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedBigRouterLimitExceeded (709) Type: cpamLicensingAlarm Package: security.LicensedBigRouterLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of Nokia large routers in the network reaches 100 percent of the 5650 CPAM license capacity.		
Raising condition: ('isLicensedBigRouterLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedBigRouterLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Big Router licenses purchased and available on the CPAM server is insufficient as compared to the number of big routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-427 LicensedBigRouterLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedBigRouterLimitNearing (710) Type: cpamLicensingAlarm Package: security.LicensedBigRouterLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of Nokia large routers in the network reaches 75 to 90 percent of the 5650 CPAM license capacity.		
Remedial action: Informational - The number of Big Router licenses purchased and available on the CPAM server is insufficient as compared to the number of big routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-428 LicensedBigRouterLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedBigRouterLimitNearlyExceeded (711) Type: cpamLicensingAlarm Package: security. LicensedBigRouterLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of Nokia large routers in the network reaches 90 to 100 percent of the 5650 CPAM license capacity.		
Remedial action: Informational - The number of Big Router licenses purchased and available on the CPAM server is insufficient as compared to the number of big routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-429 LicensedCpaaLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedCpaaLimitExceeded (389) Type: cpamLicensingAlarm Package: security.LicensedCpaaLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of 7701 CPAAs in the network reaches 100 percent of the license capacity.		
Raising condition: ('isLicensedCpaaLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedCpaaLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of CPAA licenses purchased and available on the CPAM server is insufficient as compared to the number of CPAAs under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-430 LicensedCpaaLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedCpaaLimitNearing (390) Type: cpamLicensingAlarm Package: security.LicensedCpaaLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of 7701 CPAAs in the network reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of CPAA licenses purchased and available on the CPAM server is insufficient as compared to the number of CPAAs under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-431 LicensedCpaaLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedCpaaLimitNearlyExceeded (391) Type: cpamLicensingAlarm Package: security.LicensedCpaaLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of 7701 CPAAs in the network reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of CPAA licenses purchased and available on the CPAM server is insufficient as compared to the number of CPAAs under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-432 LicensedImpactAnalysisRouterLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedImpactAnalysisRouterLimitExceeded (712) Type: cpamLicensingAlarm Package: security. LicensedImpactAnalysisRouterLimitExceeded Raised on class: security.CpamLicenseScenario	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of routers in a simulation scenario reaches 100 percent of the license capacity.		
Raising condition: ('isLicensedRouterLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedRouterLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of licenses purchased and available on the CPAM server for routers in a simulation scenario is insufficient as compared to the number of routers in a simulation scenario. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-433 LicensedImpactAnalysisRouterLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedImpactAnalysisRouterLimitNearing (713) Type: cpamLicensingAlarm Package: security.LicensedImpactAnalysisRouterLimitNearing Raised on class: security.CpamLicenseScenario	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of routers in a simulation scenario reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of licenses purchased and available on the CPAM server for routers in a simulation scenario is insufficient as compared to the number of routers in a simulation scenario. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-434 LicensedImpactAnalysisRouterLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedImpactAnalysisRouter-LimitNearlyExceeded (714) Type: cpamLicensingAlarm Package: security.LicensedImpactAnalysisRouterLimitNearlyExceeded Raised on class: security.CpamLicenseScenario	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of routers in a simulation scenario reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of licenses purchased and available on the CPAM server for routers in a simulation scenario is insufficient as compared to the number of routers in a simulation scenario. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-435 LicensedIpPathLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedIpPathLimitExceeded (715) Type: cpamLicensingAlarm Package: security.LicensedIpPathLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 100 percent of the license capacity.		
Raising condition: ('isLicensedIpPathLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedIpPathLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Path Computation Module licenses purchased and available on the CPAM server is insufficient as compared to the number of PCA paths in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-436 LicensedIpPathLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedIpPathLimitNearing (716) Type: cpamLicensingAlarm Package: security.LicensedIpPathLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of Path Computation Module licenses purchased and available on the CPAM server is insufficient as compared to the number of PCA paths in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-437 LicensedIpPathLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedIpPathLimitNearlyExceeded (717) Type: cpamLicensingAlarm Package: security. LicensedIpPathLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of IP path monitors in the 5650 CPAM reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of Path Computation Module licenses purchased and available on the CPAM server is insufficient as compared to the number of PCA paths in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-438 LicensedLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedLimitNearing (1931) Type: licensingAlarm Package: security.LicensedLimitNearing Raised on class: security.SamLicensePoints	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitNearing	Release: • N/A
Description: The alarm is raised when the license items in the network reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-439 LicensedLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitNearlyExceeded (1932) Type: licensingAlarm Package: security.LicensedLimitNearlyExceeded Raised on class: security.SamLicensePoints	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the license items in the network reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-440 LicensedLimitReached

Alarm	Attributes	Applicable major release
Name: LicensedLimitReached (1933) Type: licensingAlarm Package: security.LicensedLimitReached Raised on class: security.SamLicensePoints	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitReached	Release: • N/A
Description: The alarm is raised when the license items in the network reaches 100 percent of the license capacity.		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-441 LicensedMcRouterLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedMcRouterLimitExceeded (718) Type: cpamLicensingAlarm Package: security.LicensedMcRouterLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 100 percent of the license capacity.		
Raising condition: ('isLicensedMcRouterLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedMcRouterLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Multicast Router licenses purchased and available on the CPAM server is insufficient as compared to the number of multicast routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-442 LicensedMcRouterLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedMcRouterLimitNearing (719) Type: cpamLicensingAlarm Package: security.LicensedMcRouterLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 75 to 90 percent of the license capacity.		
Remedial action: Informational - The number of Multicast Router licenses purchased and available on the CPAM server is insufficient as compared to the number of multicast routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-443 LicensedMcRouterLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedMcRouterLimitNearlyExceeded (720) Type: cpamLicensingAlarm Package: security. LicensedMcRouterLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of multicast routers in the 5650 CPAM reaches 90 to 100 percent of the license capacity.		
Remedial action: Informational - The number of Multicast Router licenses purchased and available on the CPAM server is insufficient as compared to the number of multicast routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-444 LicensedSmallRouterLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedSmallRouterLimitExceeded (727) Type: cpamLicensingAlarm Package: security.LicensedSmallRouterLimitExceeded Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of Nokia small routers in the network reaches 100 percent of the 5650 CPAM license capacity.		
Raising condition: ('isLicensedSmallRouterLimitExceeded' EQUAL 'true')		
Clearing condition: ('isLicensedSmallRouterLimitExceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of Small Router licenses purchased and available on the CPAM server is insufficient as compared to the number of small routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-445 LicensedSmallRouterLimitNearing

Alarm	Attributes	Applicable major release
Name: LicensedSmallRouterLimitNearing (728) Type: cpamLicensingAlarm Package: security.LicensedSmallRouterLimitNearing Raised on class: security.CpamLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearing	Release: • N/A
Description: The alarm is raised when the number of Nokia small routers in the network reaches 75 to 90 percent of the 5650 CPAM license capacity.		
Remedial action: Informational - The number of Small Router licenses purchased and available on the CPAM server is insufficient as compared to the number of small routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-446 LicensedSmallRouterLimitNearlyExceeded

Alarm	Attributes	Applicable major release
Name: LicensedSmallRouterLimitNearlyExceeded (729) Type: cpamLicensingAlarm Package: security. LicensedSmallRouterLimitNearlyExceeded Raised on class: security.CpamLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamLicensedLimitNearlyExceeded	Release: • N/A
Description: The alarm is raised when the number of Nokia small routers in the network reaches 90 to 100 percent of the 5650 CPAM license capacity.		
Remedial action: Informational - The number of Small Router licenses purchased and available on the CPAM server is insufficient as compared to the number of small routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-447 licenseExpiration

Alarm	Attributes	Applicable major release
Name: licenseExpiration (2911) Type: configurationAlarm Package: ranlicense.licenseExpiration Raised on class: ranlicense.RANLicense	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licenseExpired	Release: • N/A
Description: The alarm is raised when a RAN license expires.		
Remedial action: Provide a new LKDI license file with a further expiration date.		

Table 39-448 LicenseKeyIsInvalid

Alarm	Attributes	Applicable major release
Name: LicenseKeyIsInvalid (1122) Type: licensingAlarm Package: security.LicenseKeyIsInvalid Raised on class: security.AbstractLicense	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LicenseKeyIsInvalid	Release: • N/A
Description: The alarm is raised when the 5620 SAM server configuration is updated with a new license key and the license key is not valid.		
Remedial action: Informational - The license key information entered is invalid. Please re-enter the license key information. If the alarm persists contact your Nokia support representative for assistance.		

Table 39-449 LicenseMismatch

Alarm	Attributes	Applicable major release
Name: LicenseMismatch (342) Type: licensingAlarm Package: security.LicenseMismatch Raised on class: security.AbstractLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: licenseMismatch	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM main server license does not match the standby 5620 SAM main server license.		
Remedial action: Informational - Please ensure that the same license key is installed on both the active and standby SAM/CPAM servers		

Table 39-450 LicenseMisMatch

Alarm	Attributes	Applicable major release
Name: LicenseMisMatch (693) Type: cpamLicensingAlarm Package: security.LicenseMisMatch Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: cpamLicenseMisMatch	Release: • N/A
Description: The alarm is raised when the primary 5650 CPAM server license does not match the standby 5650 CPAM server license.		
Remedial action: Informational - Please ensure that the same license key is installed on both the active and standby SAM/CPAM servers		

Table 39-451 LicenseUpgradeFailed

Alarm	Attributes	Applicable major release
Name: LicenseUpgradeFailed (4389) Type: configurationAlarm Package: nelicense.LicenseUpgradeFailed Raised on class: nelicense.LicenseUpgradeStatus	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileAccessError	Release: • N/A
Description: The alarm is raised when an NE license upgrade using the 5620 SAM fails.		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues. Invalid License File.		

Table 39-452 LicenseViolation

Alarm	Attributes	Applicable major release
Name: LicenseViolation (1930) Type: licensingAlarm Package: security.LicenseViolation Raised on class: security.SamLicensePoints	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licenseViolation Applicable probable causes: • licenseViolation • HostIdUsedInsteadOfUUIDForX86	Release: • N/A
Description: The alarm is raised when a license violation has occurred. Alarms raised against licensed products, due to the licensed product limit being zero at the time of node discovery, will be implicitly cleared if a new license that sets the licensed product limit to not zero is imported.		
Remedial action: Informational - the additional text field of the alarm will provide more details. If the alarm persists contact your Nokia sales representative to purchase additional licenses.		

Table 39-453 licenseViolation

Alarm	Attributes	Applicable major release
Name: licenseViolation (2912) Type: configurationAlarm Package: ranlicense.licenseViolation Raised on class: ranlicense.RANLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: noMoreTokens	Release: • N/A
Description: The alarm is raised when a RAN license is in violation due to insufficient tokens.		
Remedial action: Provide a new LKDI license file with more tokens.		

Table 39-454 liDestinationChangeReject

Alarm	Attributes	Applicable major release
Name: liDestinationChangeReject (551) Type: ConfigurationAlarm Package: mirrorli.liDestinationChangeReject Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorDestinationChangeReject	Release: • N/A
Description: The alarm is raised when an operator tries to modify a mirror destination that is in use by an LI mirror.		
Remedial action: Informational - no corrective action required.		

Table 39-455 liDestinationEnabled

Alarm	Attributes	Applicable major release
Name: liDestinationEnabled (550) Type: ConfigurationAlarm Package: mirrorli.liDestinationEnabled Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorDestinationEnabled	Release: • N/A
Description: The alarm is raised when a mirror destination Operational State changes from Down to Up.		
Remedial action: Informational - no corrective action required.		

Table 39-456 LIF

Alarm	Attributes	Applicable major release
Name: LIF (804) Type: communicationsAlarm Package: mpr.LIF Raised on class: mpr.IMALink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfIMAFrame	Release: • N/A
Description: The alarm is raised when a Loss of IMA Frame signal is detected on an ASAP MDA.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-457 liFilterAssignToItfWarn

Alarm	Attributes	Applicable major release
Name: liFilterAssignToItfWarn (556) Type: ConfigurationAlarm Package: mirrorli.liFilterAssignToItfWarn Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorFilterAssignToItfWarn	Release: • N/A
Description: The alarm is raised when an operator tries to assign a filter that is in use by LI to an interface.		
Remedial action: Informational - no corrective action required.		

Table 39-458 liFilterAssignToSapWarn

Alarm	Attributes	Applicable major release
Name: liFilterAssignToSapWarn (554) Type: ConfigurationAlarm Package: mirrorli.liFilterAssignToSapWarn Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorFilterAssignToSapWarn	Release: • N/A
Description: The alarm is raised when an operator tries to assign a filter that is in use by LI to a SAP.		
Remedial action: Informational - no corrective action required.		

Table 39-459 liFilterAssignToSdpWarn

Alarm	Attributes	Applicable major release
Name: liFilterAssignToSdpWarn (555) Type: ConfigurationAlarm Package: mirrorli.liFilterAssignToSdpWarn Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorFilterAssignToSdpWarn	Release: • N/A
Description: The alarm is raised when an operator tries to assign a filter that is in use by LI to an SDP.		
Remedial action: Informational - no corrective action required.		

Table 39-460 LinkAggMemberMisconfigured

Alarm	Attributes	Applicable major release
Name: LinkAggMemberMisconfigured (652) Type: lnkaggAlarm Package: lag.LinkAggMemberMisconfigured Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagMemberMisconfigured	Release: • N/A
Description: The alarm is raised when one or more misconfigured LAG members are detected, for example, when some LAG members are in access mode and some are in network mode.		
Remedial action: A configuration error has occurred which must be corrected. The configuration of the LAG port member should be checked and the configuration error corrected,		

Table 39-461 LinkAggModeMisconfigured

Alarm	Attributes	Applicable major release
Name: LinkAggModeMisconfigured (653) Type: lnkaggAlarm Package: lag.LinkAggModeMisconfigured Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagModeMisconfigured	Release: • N/A

Table 39-461 LinkAggModeMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the LAG mode differs from the mode of one or more LAG members, for example, when the LAG mode is access and the LAG members are in network mode.		
Remedial action: A configuration error has occurred which must be corrected. The configuration of the LAG port member should be checked and the configuration error corrected,		

Table 39-462 LinkAggPortJoin

Alarm	Attributes	Applicable major release
Name: LinkAggPortJoin (654) Type: lnkaggAlarm Package: lag.LinkAggPortJoin Raised on class: lag.Interface	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: lagPortJoin	Release: • N/A
Description: The alarm is raised when a LAG port joins a LAG by entering the attached state.		
Remedial action: Informational.		

Table 39-463 LinkAggPortLeave

Alarm	Attributes	Applicable major release
Name: LinkAggPortLeave (655) Type: lnkaggAlarm Package: lag.LinkAggPortLeave Raised on class: lag.Interface	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: lagPortLeave	Release: • N/A
Description: The alarm is raised when a LAG port leaves a LAG by exiting the attached state.		
Remedial action: Informational.		

Table 39-464 LinkAggPortRemove

Alarm	Attributes	Applicable major release
Name: LinkAggPortRemove (656) Type: lnkaggAlarm Package: lag.LinkAggPortRemove Raised on class: lag.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: lagPortRemove	Release: • N/A
Description: The alarm is raised when a LAG port is removed from a LAG because of an invalid configuration.		
Remedial action: A configuration error has occurred which must be corrected. Please check the configuration of the port in question.		

Table 39-465 LinkDown (optical)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: optical.LinkDown Raised on class: optical.OpticalLink	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when any of the Optical Link end point is operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the Link End points to understand why the underlying transport network is unreliable.		

Table 39-466 LinkIdentifierMismatch (mwa)

Alarm	Attributes	Applicable major release
Name: LinkIdentifierMismatch (686) Type: communicationsAlarm Package: mwa.LinkIdentifierMismatch Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LinkIdentifierMismatch	Release: • N/A
Description: The alarm is raised when a MPT detects a link identifier mismatch.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-467 linkLoss

Alarm	Attributes	Applicable major release
Name: linkLoss (6389) Type: communicationsAlarm Package: femto.linkLoss Raised on class: femto.FemtoNetwork	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • N/A
Description: This alarm is deprecated from femto 16.1.		
Remedial action: See the nodal documentation for more information.		

Table 39-468 liSourceDisabled

Alarm	Attributes	Applicable major release
Name: liSourceDisabled (563) Type: ConfigurationAlarm Package: mirrorli.liSourceDisabled Raised on class: mirrorli.LISourceCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceDisabled	Release: • N/A
Description: The alarm is raised when an LI mirror source Operational State changes from Up to Down.		

Table 39-468 liSourceDisabled (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 39-469 liSourceEnabled

Alarm	Attributes	Applicable major release
Name: liSourceEnabled (562) Type: ConfigurationAlarm Package: mirrorli.liSourceEnabled Raised on class: mirrorli.LISourceCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceEnabled	Release: • N/A
Description: The alarm is raised when an LI mirror source Operational State changes from Down to Up.		
Remedial action: Informational - no corrective action required.		

Table 39-470 liSourceFilterAssignReject

Alarm	Attributes	Applicable major release
Name: liSourceFilterAssignReject (557) Type: ConfigurationAlarm Package: mirrorli.liSourceFilterAssignReject Raised on class: mirrorli.LIMgmtSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceFilterAssignReject	Release: • N/A
Description: The alarm is raised when an operator tries to modify a filter that is in use by LI.		
Remedial action: Informational - no corrective action required.		

Table 39-471 liSourceFilterAssignWarn

Alarm	Attributes	Applicable major release
Name: liSourceFilterAssignWarn (559) Type: ConfigurationAlarm Package: mirrorli.liSourceFilterAssignWarn Raised on class: mirrorli.LIMgmtSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceFilterAssignWarn	Release: • N/A
Description: The alarm is raised when an operator assigns a mirror filter that is in use by LI and the assignment may be overruled.		
Remedial action: Informational - no corrective action required.		

Table 39-472 liSourceFilterChanged

Alarm	Attributes	Applicable major release
Name: liSourceFilterChanged (3313) Type: ConfigurationAlarm Package: mirrorli.liSourceFilterChanged Raised on class: mirrorli.LIMgmtSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceLiFilterChanged	Release: • N/A
Description: The alarm is raised when a parameter of a filter which is referenced by Lawful Intercept (LI), or a parameter of one of its entry is changed. This notification may be triggered only if the LI filter lock is overruled, and one of the following actions occurs: -a filter referenced by LI has been deleted. -one of the parameters (default-action, scope) of a filter which is referenced by LI has been changed. -a filter which is referenced by LI is overwritten. -a new entry is created for a filter which is referenced by LI. -an entry of a filter which is referenced by LI is activated. -an entry is removed from a filter which is referenced by LI. -an entry of a filter which is referenced by LI is renumbered. -one of the parameters of an entry in a filter which is referenced by LI is changed.		
Remedial action: Informational - no corrective action required.		

Table 39-473 liSourceFilterOverruled

Alarm	Attributes	Applicable major release
Name: liSourceFilterOverruled (558) Type: ConfigurationAlarm Package: mirrorli.liSourceFilterOverruled Raised on class: mirrorli.LIMgmtSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceFilterOverruled	Release: • N/A
Description: The alarm is raised when the assignment of a mirror filter is overruled by another filter assignment.		
Remedial action: Informational - no corrective action required.		

Table 39-474 liSourceIP6FltrChangeReject

Alarm	Attributes	Applicable major release
Name: liSourceIP6FltrChangeReject (4377) Type: ConfigurationAlarm Package: mirrorli.liSourceIP6FltrChangeReject Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceIP6FltrChangeReject	Release: • N/A
Description: The alarm is raised when an operator tries to modify an IPv6 filter or an IPv6 filter entry that is in use by LI.		
Remedial action: Informational - no corrective action required.		

Table 39-475 liSourceIPFltrChangeReject

Alarm	Attributes	Applicable major release
Name: liSourceIPFltrChangeReject (552) Type: ConfigurationAlarm Package: mirrorli.liSourceIPFltrChangeReject Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceIPFltrChangeReject	Release: • N/A
Description: The alarm is raised when an operator tries to modify an IP filter or an IP filter entry that is in use by LI.		
Remedial action: Informational - no corrective action required.		

Table 39-476 liSourceMacFltrChangeReject

Alarm	Attributes	Applicable major release
Name: liSourceMacFltrChangeReject (553) Type: ConfigurationAlarm Package: mirrorli.liSourceMacFltrChangeReject Raised on class: mirrorli.LIMirrorSiteCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceMacFltrChangeReject	Release: • N/A
Description: The alarm is raised when an operator tries to modify a MAC filter or a MAC filter entry that is in use by LI.		
Remedial action: Informational - no corrective action required.		

Table 39-477 liSourceSapChange

Alarm	Attributes	Applicable major release
Name: liSourceSapChange (560) Type: ConfigurationAlarm Package: mirrorli.liSourceSapChange Raised on class: mirrorli.LISourceInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceSapChange	Release: • N/A
Description: The alarm is raised when a SAP that is associated with LI is modified or deleted.		
Remedial action: Informational - no corrective action required.		

Table 39-478 liSourceSubscriberChange

Alarm	Attributes	Applicable major release
Name: liSourceSubscriberChange (561) Type: ConfigurationAlarm Package: mirrorli.liSourceSubscriberChange Raised on class: mirrorli.LISourceSubscriberHost	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceSubChange	Release: • N/A
Description: The alarm is raised when a subscriber that is associated with LI is modified or deleted.		

Table 39-478 liSourceSubscriberChange (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 39-479 LODS

Alarm	Attributes	Applicable major release
Name: LODS (805) Type: communicationsAlarm Package: mpr.LODS Raised on class: mpr.IMALink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfDelaySynchronization	Release: • N/A
Description: The alarm is raised when a Loss of Delay Synchronization signal is detected on an ASAP MDA.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-480 LogLocFailure

Alarm	Attributes	Applicable major release
Name: LogLocFailure (340) Type: storageAlarm Package: file.LogLocFailure Raised on class: file.Policy	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AdminLocFailure Applicable probable causes: • AdminLocFailure • BackupLocFailure	Release: • N/A
Description: The alarm is raised when an attempt to create a log or billing file fails. The probable cause is AdminLocFailure when using the admin location fails, in which case the backup location, if specified, is used. The probable cause is BackupLocFailure when using the backup location fails.		
Remedial action: The flash device targeted to store the log or billing file is either full or the directory does not exist. An analysis of the files on the flash device needs to be analyzed and redundant files removed or the directory must be configured. Log into the NE via the CLI to perform the cleanup/creation operations.		

Table 39-481 LossOfAlignment

Alarm	Attributes	Applicable major release
Name: LossOfAlignment (629) Type: communicationsAlarm Package: equipment.LossOfAlignment Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfAlignment	Release: • N/A
Description: The alarm is raised when a Loss of Alignment signal is detected.		

Table 39-481 LossOfAlignment (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-482 LossOfESMC

Alarm	Attributes	Applicable major release
Name: LossOfESMC (2939) Type: communicationsAlarm Package: equipment.LossOfESMC Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfESMC	Release: • N/A
Description: The alarm is raised when a loss of ESMC signal failure is detected.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-483 LossOfPointer

Alarm	Attributes	Applicable major release
Name: LossOfPointer (3623) Type: communicationsAlarm Package: equipment.LossOfPointer Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfPointer	Release: • N/A
Description: The alarm is raised when a loss of pointer occurs		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-484 LossOfPointerHOPath

Alarm	Attributes	Applicable major release
Name: LossOfPointerHOPath (9007) Type: communicationsAlarm Package: tdm.LossOfPointerHOPath Raised on class: tdm.AUn	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LOPP	Release: • N/A
Description: The alarm is raised on Loss of Pointer HO Path (NEND).		

Table 39-484 LossOfPointerHOPath (continued)

Alarm	Attributes	Applicable major release
Remedial action: Loss of Pointer found on HO Path at NEND.		

Table 39-485 LossOfRadioFrame

Alarm	Attributes	Applicable major release
Name: LossOfRadioFrame (4828) Type: communicationsAlarm Package: mwa.LossOfRadioFrame Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfFrame	Release: • N/A
Description: The alarm is raised when a MPT detects a Loss of Radio Frame from Radio Path		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-486 LossOfRadioFramesAlignment

Alarm	Attributes	Applicable major release
Name: LossOfRadioFramesAlignment (4829) Type: communicationsAlarm Package: mwa.LossOfRadioFramesAlignment Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfAlignment	Release: • N/A
Description: The alarm is raised when a MPT detects a Loss of Radio Frames Alignment		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-487 LowSwitchFabricCap

Alarm	Attributes	Applicable major release
Name: LowSwitchFabricCap (5178) Type: hardwareAnomaly Package: equipment.LowSwitchFabricCap Raised on class: equipment.Card	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LowSwitchFabricCapacity	Release: • N/A
Description: The alarm is raised when the total switch fabric capacity becomes less than the line card capacity due to link failures. At least one of the taps on the Card is below 100% capacity.		
Remedial action: 1. Make sure that the hardware switching fabric capacity is more than the line card capacity. 2. Please reboot the card and check if it resolves the problem. If problem persists after reboot, please contact your Nokia support representative for assistance.		

Table 39-488 LpsLearnMac

Alarm	Attributes	Applicable major release
Name: LpsLearnMac (519) Type: learnedPortSecurityAlarm Package: lps.LpsLearnMac Raised on class: lps.LearnedPortSecurity	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLearnedBridgedMAC	Release: • N/A
Description: The alarm is raised when an LPS port learns a bridged MAC address.		
Remedial action: Informational - no corrective action required.		

Table 39-489 LpsPortUpAfterLearningWindowExpired

Alarm	Attributes	Applicable major release
Name: LpsPortUpAfterLearningWindowExpired (517) Type: learnedPortSecurityAlarm Package: lps.LpsPortUpAfterLearningWindowExpired Raised on class: lps.LPSConfiguration	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portUpAfterLearningWin-dowExpired	Release: • N/A
Description: The alarm is raised either when an LPS port is enabled after the learning window expires and MAC address learning on the port is disabled, or when the learning window expires with slice and port values of 0.		
Remedial action: Informational - no corrective action required.		

Table 39-490 LsdbOverflow

Alarm	Attributes	Applicable major release
Name: LsdbOverflow (53) Type: equipmentAlarm Package: ospf.LsdbOverflow Raised on class: ospf.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceFull	Release: • N/A
Description: The alarm is raised when the number of received external LSAs exceeds the configured number allowed. By default, there is no limit. The alarm information includes the configured LSDB limit and one of the following LSDB overflow states: - 0, which means no overflow - 1, which means nearing limit - 2, which means limit exceeded		
Remedial action: Informational - the number of received external LSAs exceeds the configured number allowed. The alarm will also be raised when external LSAs is nearing limit.		

Table 39-491 LudbDhcpHostGroupIfTooLong

Alarm	Attributes	Applicable major release
Name: LudbDhcpHostGroupIfTooLong (4627) Type: LudbDhcpHostGroupIfTooLongAlarm Package: localuserdb.LudbDhcpHostGroupIfTooLong Raised on class: localuserdb.DhcpHost	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ludbDhcpHostGroupIfTooLong	Release: • N/A
Description: The alarm is raised when the default MSAP group interface name of a DHCP Host, concatenated with the port ID is longer than 32 characters.		
Remedial action: The string configured in DHCP Host as default MSAP Group Interface Name concatenated with the port-id is longer than 32 characters. It is an invalid configuration since it exceeds the length allowed for a Group Interface Name. (Please) Reconfigure the MSAP Group Interface Name or refer to the Local User Database documentation for assistance.		

Table 39-492 LudbPppHostGroupIfTooLong

Alarm	Attributes	Applicable major release
Name: LudbPppHostGroupIfTooLong (4628) Type: LudbPppHostGroupIfTooLongAlarm Package: localuserdb.LudbPppHostGroupIfTooLong Raised on class: localuserdb.PppHost	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ludbPppHostGroupIfTooLong	Release: • N/A
Description: The alarm is raised when the default MSAP group interface name of a PPP host, concatenated with the port ID is longer than 32 characters.		
Remedial action: The string configured in PPP Host as default MSAP Group Interface Name concatenated with the port-id is longer than 32 characters. It is an invalid configuration since it exceeds the length allowed for a Group Interface Name. (Please) Reconfigure the MSAP Group Interface Name or refer to the Local User Database documentation for assistance.		

Table 39-493 MacAccountingLimitReached (rtr)

Alarm	Attributes	Applicable major release
Name: MacAccountingLimitReached (4907) Type: macAccountingAlarm Package: rtr.MacAccountingLimitReached Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: macAccountingLimitReached	Release: • N/A
Description: The alarm is raised when the system detects that the MAC accounting table is full.		
Remedial action: This alarm can be cleared when the used MAC entries are deleted by disabling MAC accounting on a particular interface or through manual intervention with a user command such as clear router interface mac.		

Table 39-494 MacAccountingLimitReached (service)

Alarm	Attributes	Applicable major release
Name: MacAccountingLimitReached (4907) Type: macAccountingAlarm Package: service.MacAccountingLimitReached Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: macAccountingLimitReached	Release: • N/A
Description: The alarm is raised when the system detects that the MAC accounting table is full.		
Remedial action: This alarm can be cleared when the used MAC entries are deleted by disabling MAC accounting on a particular interface or through manual intervention with a user command such as clear router interface mac.		

Table 39-495 macMoveRateExceededNonBlock (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceededNonBlock (4893) Type: accessInterfaceAlarm Package: service.macMoveRateExceededNonBlock Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MacMoveRateExceededNon-Block	Release: • N/A
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site when limitMacMove(sapTlsLimit-MacMove) is set to 'nonBlocking'.		
Remedial action: Informational - User can adjust the value of 'MAC Move Maximum Rate' to reduce the frequency of this alarm.		

Table 39-496 MacPinningViolation

Alarm	Attributes	Applicable major release
Name: MacPinningViolation (443) Type: serviceAlarm Package: vpls.MacPinningViolation Raised on class: vpls.AbstractSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: macAddressPinned	Release: • N/A
Description: The alarm is raised when an attempt is made to assign a pinned MAC address to another L2 access interface or spoke SDP binding in an M-VPLS or VPLS.		
Remedial action: Use a MAC address that is not already pinned.		

Table 39-497 ManagedRouteAddFailed

Alarm	Attributes	Applicable major release
Name: ManagedRouteAddFailed (5130) Type: processingErrorAlarm Package: rtr.ManagedRouteAddFailed Raised on class: rtr.RoutingInstanceSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxVRtrManagedRouteAdd-Failed	Release: • N/A
Description: The alarm is raised when a managed route could not be installed.		
Remedial action: Check the additional text of the alarm for more details.		

Table 39-498 ManagedRouteFailedRetryThresholdCrossed

Alarm	Attributes	Applicable major release
Name: ManagedRouteFailedRetryThresholdCrossed (397) Type: topologyAlarm Package: topology. ManagedRouteFailedRetryThresholdCrossed Raised on class: topology.RouteManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: managedRouteCouldNot-BeSetup	Release: • N/A
Description: The alarm is raised when the 5650 CPAM cannot set up a managed route after the number of attempts specified by the cpamManagedRoute problematicThresholdAlarmAfter value in the nms-server.xml file. The alarm is raised if the cpamManagedRoute problematicRetryStrategy value in nms-server.xml is set to countdown. The alarm is not raised if the problematicRetryStrategy value is set to the default of reactive.		
Remedial action: Informational - The Retry strategy can be modified in nms-server.xml. This alarm is not raised for the default retry strategy, reactive.		

Table 39-499 ManagedRouteRetryAttemptsExhausted

Alarm	Attributes	Applicable major release
Name: ManagedRouteRetryAttemptsExhausted (398) Type: topologyAlarm Package: topology. ManagedRouteRetryAttemptsExhausted Raised on class: topology.RouteManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: managedRouteCouldNot-BeSetup	Release: • N/A
Description: The alarm is raised when the 5650 CPAM stops trying to set up a managed route after the number of attempts specified by the cpamManagedRoute problematicDeadAfter value in the nms-server.xml file. The alarm is raised if the cpamManagedRoute problematicRetryStrategy value in nms-server.xml is set to countdown. The alarm is not raised if the problematicRetryStrategy value is set to the default value of reactive.		
Remedial action: Informational - The Retry strategy can be modified in nms-server.xml. This alarm is not raised for the default retry strategy, reactive.		

Table 39-500 ManagementAccessFilterMisconfigured

Alarm	Attributes	Applicable major release
Name: ManagementAccessFilterMisconfigured (76) Type: configurationAlarm Package: sitesec.ManagementAccessFilterMisconfigured Raised on classes: • sitesec.MafEntry • sitesec.MacMafEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidSourcePortIdentifier	Release: • N/A
Description: The alarm is raised when a MAF is misconfigured.		
Raising condition: ('isValidSourcePortName' EQUAL 'false')		
Clearing condition: ('isValidSourcePortName' EQUAL 'true')		
Remedial action: A configuration error has occurred which must be corrected. Please check the management access filter configuration for errors.		

Table 39-501 ManagementAccessFilterMisconfiguredIpv6

Alarm	Attributes	Applicable major release
Name: ManagementAccessFilterMisconfiguredIpv6 (1112) Type: configurationAlarm Package: sitesec. ManagementAccessFilterMisconfiguredIpv6 Raised on class: sitesec.MafIPv6Entry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidSourcePortIdentifier	Release: • N/A
Description: The alarm is raised when an IPv6 MAF is misconfigured.		
Raising condition: ('isValidSourcePortName' EQUAL 'false')		
Clearing condition: ('isValidSourcePortName' EQUAL 'true')		
Remedial action: A configuration error has occurred which must be corrected. Please check the management access filter configuration for errors.		

Table 39-502 ManagementInterfaceProtectionSwitch

Alarm	Attributes	Applicable major release
Name: ManagementInterfaceProtectionSwitch (34) Type: communicationsAlarm Package: netw.ManagementInterfaceProtectionSwitch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: switchToInband Applicable probable causes: • switchToInband • switchToOutband	Release: • N/A

Table 39-502 ManagementInterfaceProtectionSwitch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE has in-band and out-of-band management interfaces and switches from one type of management to the other.		
Remedial action: Informational		

Table 39-503 ManagementIpAddressMismatch

Alarm	Attributes	Applicable major release
Name: ManagementIpAddressMismatch (1943) Type: communicationsAlarm Package: netw.ManagementIpAddressMismatch Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchOfManagementIpAddress	Release: • N/A
Description: The alarm is raised when the IP address of the shadow network element does not match with the IP address of the discovered NE.		
Remedial action: A configuration error has been made which must be corrected. One of 2 scenario is possible a) the IP address assigned to the shadow NE is incorrect or the IP address configured on the NE itself is incorrect.		

Table 39-504 ManagementIPSwitchUnsupported

Alarm	Attributes	Applicable major release
Name: ManagementIPSwitchUnsupported (1078) Type: communicationsAlarm Package: netw.ManagementIPSwitchUnsupported Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: managementAddressInvalid	Release: • N/A
Description: The alarm is raised when an attempt is made to switch the management address of an NE from one IP version to another.		
Remedial action: The additional text field of the alarm will provide guidance as to the reason for the failure - the most probable cause is a configuration error. The configuration error must be corrected. Once the issue has been resolved SAM will automatically re-attempt.		

Table 39-505 ManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: ManagementVlanConflict (215) Type: configurationAlarm Package: vlan.ManagementVlanConflict Raised on class: vlan.Vlan	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • N/A
Description: The alarm is raised when a management VLAN ID is in use by another service type.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		

Table 39-505 ManagementVlanConflict (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service is not used on any other type of VLAN Service.		

Table 39-506 ManualCpaaSwitchover

Alarm	Attributes	Applicable major release
Name: ManualCpaaSwitchover (5143) Type: configurationAlarm Package: topology.ManualCpaaSwitchover Raised on class: topology.Cpaa	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CPAASwitchover	Release: • N/A
Description: The alarm is raised when an operator has manually initiated a switchover. This alarm is not self clearing. Another switchover will not be permitted for 10 mins.		
Remedial action: Manual Switchover has been executed.		

Table 39-507 ManualManagementRemoval

Alarm	Attributes	Applicable major release
Name: ManualManagementRemoval (9008) Type: equipmentAlarm Package: tdm.ManualManagementRemoval Raised on class: tdm.AUn	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MAN	Release: • N/A
Description: The alarm is raised on Manual (Management) Removal (NEND).		
Remedial action: AUn facility is manually (Management) Removed at NEND.		

Table 39-508 MaxExecutingScripts

Alarm	Attributes	Applicable major release
Name: MaxExecutingScripts (3686) Type: serverAlarm Package: script.MaxExecutingScripts Raised on class: script.AbstractScript	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: maxExecutingScripts	Release: • N/A
Description: The alarm is raised when the maximum number of scripts allowed to execute concurrently is exceeded.		
Remedial action: The number of being scripts executed simultaneously has exceeded to maximum allowed. Reduce the number of scripts being executed. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-509 MaxFecLimitReached

Alarm	Attributes	Applicable major release
Name: MaxFecLimitReached (6448) Type: processingErrorAlarm Package: ldp.MaxFecLimitReached Raised on class: ldp.Peer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxFecLimitReached	Release: • N/A
Description: The alarm is raised when the number of FECs accepted from the peer has reached the value specified by fecLimit. The alarm is cleared when a new MaxFecThresholdChange notification is received.		
Remedial action: Number of FECs accepted from the peer has reached the value specified by FEC Limit. Appropriate configuration changes in local or peer LSR will be required.		

Table 39-510 MaxFecThresholdChange

Alarm	Attributes	Applicable major release
Name: MaxFecThresholdChange (6449) Type: processingErrorAlarm Package: ldp.MaxFecThresholdChange Raised on class: ldp.Peer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxFecThresholdChange	Release: • N/A
Description: The alarm is raised when the number of FECs accepted from the peer has exceeded the threshold percent of the value specified by fecLimit. The alarm is cleared when the number of FECs received drops below the threshold percent of the value specified by fecLimit.		
Remedial action: Number of FECs accepted from the peer has exceeded or dropped below the threshold percent of the value specified by FEC Limit. Appropriate configuration changes in local or peer LSR will be required.		

Table 39-511 MaxNumExportRoutesReached

Alarm	Attributes	Applicable major release
Name: MaxNumExportRoutesReached (1116) Type: ProtocolAlarm Package: vprn.MaxNumExportRoutesReached Raised on class: vprn.AbstractSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxNumExportRoutes-Reached	Release: • N/A
Description: The alarm is raised when the number of routes exported from a route table to a VRF reaches the configured maximum.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE or VRF instance in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-512 MaxNumIpv6RoutesReached

Alarm	Attributes	Applicable major release
Name: MaxNumIpv6RoutesReached (505) Type: ProtocolAlarm Package: l3fwd.MaxNumIpv6RoutesReached Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxNumIpv6RouteReached	Release: • N/A
Description: The alarm is raised when the number of IPv6 routes in a VPRN exceeds the configured maximum.		
Remedial action: The number of IPv6 routes has exceeded the configured maximum for the VPRN - the route table must be examined to ensure that all of the routes in the table are valid and not the result of a misconfiguration in the VPRN service. If all of the routes appear to be valid then the value used as the maximum value should be revisited.		

Table 39-513 MaxNumMcastRoutes

Alarm	Attributes	Applicable major release
Name: MaxNumMcastRoutes (206) Type: ProtocolAlarm Package: l3fwd.MaxNumMcastRoutes Raised on class: l3fwd.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxNumMcastRoutes-Reached	Release: • N/A
Description: The alarm is raised when the number of multicast routes in a VPRN exceeds the configured maximum.		
Remedial action: Informational. The number of multicast routes in a VPRN exceeds the configured maximum. The value used as the threshold value should be revisited.		

Table 39-514 MaxNumRoutesReached

Alarm	Attributes	Applicable major release
Name: MaxNumRoutesReached (1198) Type: ProtocolAlarm Package: l3fwd.MaxNumRoutesReached Raised on class: l3fwd.ServiceSite	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MaxNumRoutesReached	Release: • N/A
Description: The alarm is raised when the number of routes in a VPRN reaches the maximum number of routes specified in the VPRN configuration. The alarm information includes the number of routes, the specified maximum, and the route type, which is either IPv4 or IPv6.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE or VRF instance in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-515 MaxNumV6ExportRoutesReached

Alarm	Attributes	Applicable major release
Name: MaxNumV6ExportRoutesReached (4398) Type: ProtocolAlarm Package: vprn.MaxNumV6ExportRoutesReached Raised on class: vprn.AbstractSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MaxNumV6ExportRoutesReached	Release: • N/A
Description: The alarm is raised when the number of IPv6 routes exported from a route table to a VRF reaches the configured maximum.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE or VRF instance in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-516 McacPolicyDropped (igmp)

Alarm	Attributes	Applicable major release
Name: McacPolicyDropped (341) Type: communicationsAlarm Package: igmp.McacPolicyDropped Raised on class: igmp.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpGroupOnSapDropped	Release: • N/A
Description: The alarm is raised when an IGMP group is dropped because a multicast CAC policy is applied.		
Remedial action: Informational - no corrective action required.		

Table 39-517 McacPolicyDropped (vpls)

Alarm	Attributes	Applicable major release
Name: McacPolicyDropped (341) Type: communicationsAlarm Package: vpls.McacPolicyDropped Raised on class: vpls.L2AccessInterfaceIgmpSnpgCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpGroupOnSapDropped	Release: • N/A
Description: The alarm is raised when an IGMP group is removed from a SAP because a multicast CAC policy is applied.		
Remedial action: Informational only.		

Table 39-518 McacPolicyDropped (pim)

Alarm	Attributes	Applicable major release
Name: McacPolicyDropped (341) Type: communicationsAlarm Package: pim.McacPolicyDropped Raised on class: pim.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: pimGroupOnSapDropped	Release: • N/A
Description: The alarm is raised when a PIM group is dropped because a multicast CAC policy is applied.		
Remedial action: Informational only.		

Table 39-519 McacPolicyDropped (svt)

Alarm	Attributes	Applicable major release
Name: McacPolicyDropped (341) Type: communicationsAlarm Package: svt.McacPolicyDropped Raised on class: svt.SdpBindingIgmpSnpgCfg	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpGroupOnSdpBind-Dropped	Release: • N/A
Description: The alarm is raised when an IGMP group is dropped because a multicast CAC policy is applied to an SDP binding.		
Remedial action: Informational only.		

Table 39-520 McastRoutesMidLevelThresholdReached

Alarm	Attributes	Applicable major release
Name: McastRoutesMidLevelThresholdReached (207) Type: ProtocolAlarm Package: l3fwd. McastRoutesMidLevelThresholdReached Raised on class: l3fwd.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MidLevelThresholdReached	Release: • N/A
Description: The alarm is raised when the number of multicast routes in a VPRN exceeds the configured threshold value. The alarm information includes the number of multicast routes and the threshold value.		
Remedial action: the number of multicast routes in a VPRN exceeds the configured threshold value. The value used as the threshold value should be revisited.		

Table 39-521 McIPsecTunnelGroupSyncTagMisconfigured

Alarm	Attributes	Applicable major release
Name: McIPsecTunnelGroupSyncTagMisconfigured (4817) Type: redundancyAlarm Package: multichassis.McIPsecTunnelGroupSyncTagMisconfigured Raised on class: multichassis.MultiChassisIPSecGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipsecGroupSyncTagMisconfigure	Release: • N/A
Description: The alarm is raised when a peer of MC IPsec tunnel groups has unconfigured or mismatched synchronization tag.		
Raising condition: (('Synchronization Tag' NOT EQUAL 'Synchronization Tag') OR (('Synchronization Tag' EQUAL '\"\"') OR ('Synchronization Tag' EQUAL '\"\"')))		
Clearing condition: (('Synchronization Tag' EQUAL 'Synchronization Tag') AND (('Synchronization Tag' NOT EQUAL '\"\"') AND ('Synchronization Tag' NOT EQUAL '\"\"')))		
Remedial action: Check if the synchronization tag has been configured for the MC IPsec tunnel group peer and they matches.		

Table 39-522 McLagGatewayPortDown

Alarm	Attributes	Applicable major release
Name: McLagGatewayPortDown (11241) Type: virtualPortAlarm Package: dctr.McLagGatewayPortDown Raised on class: dctr.McLagGatewayPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: McLagGatewayPortDownOrDeleted	Release: • N/A
Description: The alarm is raised when McLagGatewayPort is down.		
Raising condition: (('operationalState' NOT EQUAL '2'))		
Clearing condition: (('operationalState' EQUAL '2'))		
Remedial action: This alarm can be cleared when the MC Lag gateway virtual port is up.		

Table 39-523 McLagGatewayPortRedundancyLost

Alarm	Attributes	Applicable major release
Name: McLagGatewayPortRedundancyLost (11242) Type: virtualPortAlarm Package: dctr.McLagGatewayPortRedundancyLost Raised on class: dctr.McLagGatewayPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RedundancyVirtualPortDownOrDeleted	Release: • N/A
Description: The alarm is raised when VP is shutdown.		
Remedial action: This alarm is raised when the MC-Lag redundancy is lost for a gateway virtual port.		

Table 39-524 McLagSourceBMacLsbMisconfigured (lag)

Alarm	Attributes	Applicable major release
Name: McLagSourceBMacLsbMisconfigured (776) Type: configurationAlarm Package: lag.McLagSourceBMacLsbMisconfigured Raised on class: lag.MultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: McLagSourceBMacLsbMis-configured	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a mismatch in the last 16 bits of the source backbone MAC address on the peer device. This mismatch prevents PBB access dual homing from operating.		
Raising condition: ('srcBMacLSBMisconfigured' EQUAL 'true')		
Clearing condition: ('srcBMacLSBMisconfigured' EQUAL 'false')		
Remedial action: Check the MAC Address LSB is correct for source backbone address.		

Table 39-525 McLagSourceBMacLsbMisconfigured (multichassis)

Alarm	Attributes	Applicable major release
Name: McLagSourceBMacLsbMisconfigured (776) Type: configurationAlarm Package: multichassis. McLagSourceBMacLsbMisconfigured Raised on class: multichassis.MultiChassisLag	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: McLagSourceBMacLsbMis-configured	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a mismatch in the last 16 bits of the source backbone MAC address on the peer device. This mismatch prevents PBB access dual homing from operating.		
Raising condition: ('srcBMacLSBMisconfigured' EQUAL 'true')		
Clearing condition: ('srcBMacLSBMisconfigured' EQUAL 'false')		
Remedial action: Check the MAC Address LSB is correct for source backbone address.		

Table 39-526 McMobileGeoRedChgInfo

Alarm	Attributes	Applicable major release
Name: McMobileGeoRedChgInfo (4380) Type: equipmentAlarm Package: multichassis.McMobileGeoRedChgInfo Raised on class: multichassis. MultiChassisPeerMobileGateway	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: equipmentAlarm	Release: • N/A
Description: The alarm is raised when the mobile-gateway or the CPM has changed its geo-redundancy state or the peer's connection status has changed.		
Remedial action: Check what caused this state change. Bring the peer and/or peer-link up and ensure that the chassis and CPM geo-redundancy states are 'hot'.		

Table 39-527 McMobileIssuStateChange

Alarm	Attributes	Applicable major release
Name: McMobileIssuStateChange (5119) Type: integrityViolation Package: multichassis.McMobileIssuStateChange Raised on class: multichassis.MultiChassisPeerMobileSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchPeerSets	Release: • N/A
Description: The alarm is raised when ISSU state between the mobile-gateways participating in the geo-redundancy changes		
Remedial action: Check what caused this change in ISSU state and correct the issue for geo-redundancy to work.		

Table 39-528 McOmcrClientNumEntriesHigh

Alarm	Attributes	Applicable major release
Name: McOmcrClientNumEntriesHigh (8057) Type: communicationsAlarm Package: multichassis.McOmcrClientNumEntriesHigh Raised on class: multichassis.PeerSynchronizationProtocol	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: McOmcrClientNumEntriesHigh	Release: • N/A
Description: The alarm is raised when the system is configured as an OMCR warm standby system, and the total number of entries in the MCS database for a particular application becomes high. When the 80% and 90% threshold is crossed, there is no effect. When the 100% threshold is exceeded, the peer indicated by the values of tmnxMcPeerIpType and tmnxMcPeerIpAddr is shut down automatically by this system.		
Remedial action: Reconfigure the oversubscribed multi chassis redundancy set up to reduce the number of entries protected by this system.		

Table 39-529 McPathBlackHole

Alarm	Attributes	Applicable major release
Name: McPathBlackHole (2940) Type: resourceAlarm Package: equipment.McPathBlackHole Raised on class: equipment.DaughterCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A
Description: The alarm is raised when a multicast (S,G) specification enters a black-hole state. As of 11.0 R1, this alarm will no longer be raised. Instead, the McPathsBlackHole alarm will be raised. All existing McPathBlackHole alarms will be converted to the McPathsBlackHole on upgrade.		
Remedial action: The alarm is raised when a source, group (S,G) goes into a black-hole state. The situation may occur when a certain source, group(S,G) has a bandwidth higher than it's configured maximum and no path/plane that can accommodate for the bandwidth of the new stream. This can be remedied by increasing the path limit(iom2 and older) or plane limit (iom3 and newer) at the Daughter Card tab or by modifying Ingress Multicast Path Management policy which assigned to the card.		

Table 39-530 McPathsBlackHole

Alarm	Attributes	Applicable major release
Name: McPathsBlackHole (4903) Type: resourceAlarm Package: equipment.McPathsBlackHole Raised on class: equipment.DaughterCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceLimitReached	Release: • N/A
Description: The alarm is raised when one or more multicast (S,G) specifications enters a black-hole state.		
Remedial action: The alarm is raised when one or more source, group (S,G) goes into a black-hole state. The situation may occur when a certain source, group (S,G) has a bandwidth higher than it's configured maximum and no path/plane that can accommodate for the bandwidth of the new stream. This can be remedied by increasing the path limit(iom2 and older) or plane limit (iom3 and newer) at the Daughter Card tab or by modifying Ingress Multicast Path Management policy which assigned to the card.		

Table 39-531 McPeerOutOfSync

Alarm	Attributes	Applicable major release
Name: McPeerOutOfSync (9569) Type: communicationsAlarm Package: multichassis.McPeerOutOfSync Raised on class: multichassis. PeerSynchronizationProtocol	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PeerSyncStatusChanged	Release: • N/A
Description: The alarm is raised when the sync status of peer is OutOfSync		
Remedial action: Check the peer sync status if it is OutOfSync i.e., one of the peer is shutdown. Synchronize with the peers and the status should be inSync or SyncInProgress.		

Table 39-532 MD5AuthFailure

Alarm	Attributes	Applicable major release
Name: MD5AuthFailure (2934) Type: communicationsAlarm Package: bgp.MD5AuthFailure Raised on class: bgp.Md5Key	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: md5AuthFailure	Release: • N/A
Description: The alarm is raised when an incoming packet is dropped because of BGP MD5 key authentication failure.		
Remedial action: A configuration error has been made which must be corrected. The MD5 authentication key configured is incorrect.		

Table 39-533 MdaRuntimeEvent

Alarm	Attributes	Applicable major release
Name: MdaRuntimeEvent (9620) Type: resourceAlarm Package: equipment.MdaRuntimeEvent Raised on class: equipment.DaughterCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mdaRuntimeStatusUpdate	Release: • N/A
Description: The alarm is generated when the MDA has experienced a runtime status event worthy of reporting.		
Remedial action: Informational - no corrective action required.		

Table 39-534 MediationAuthenticationFailure (snmp)

Alarm	Attributes	Applicable major release
Name: MediationAuthenticationFailure (75) Type: communicationsAlarm Package: snmp.MediationAuthenticationFailure Raised on class: snmp.PollerManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: noMediationPolicyFound	Release: • N/A
Description: The alarm is raised when an NE has no associated 5620 SAM mediation policy.		
Remedial action: A configuration error has been made which must be corrected. Create the necessary mediation policy and associate the policy with the NE type.		

Table 39-535 MediationAuthenticationFailure (security)

Alarm	Attributes	Applicable major release
Name: MediationAuthenticationFailure (75) Type: communicationsAlarm Package: security.MediationAuthenticationFailure Raised on class: security.BaseMediationPolicy	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unsupportedSecLevel Applicable probable causes: • unsupportedSecLevel • notInTimeWindow • unknownUserName • unknownEngineID • wrongDigest • decryptionError	Release: • N/A
Description: The alarm is raised when a mediation authentication failure occurs. This alarm is in some cases automatically cleared when mediation is restored for nodes that use the same mediation policy for read, write and trap access.		
Remedial action: A configuration error has been made which must be corrected. Create the necessary mediation policy and associate the policy with the NE type.		

Table 39-536 MemoryConsumption

Alarm	Attributes	Applicable major release
Name: MemoryConsumption (216) Type: communicationsAlarm Package: netw.MemoryConsumption Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyTrapsBuffered	Release: • N/A
Description: The alarm is raised when one of the following occurs. - The number of traps from a particular NE that await processing by the 5620 SAM surpasses the NE red threshold for trap memory management in the 5620 SAM server configuration. - The global number of traps that await processing by the 5620 SAM surpasses the yellow threshold for trap memory management in the 5620 SAM server configuration. Caution: Nokia strongly recommends against modifying NE trap management threshold values; modifying these values can seriously degrade 5620 SAM performance. The alarm clears when one of the following occurs. - The number of traps from the NE that await processing falls below the NE red threshold. - The global number of traps that await processing falls below the system yellow threshold. The NE is resynchronized only if required.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

Table 39-537 MemoryThresholdCrossingAlarm

Alarm	Attributes	Applicable major release
Name: MemoryThresholdCrossingAlarm (1936) Type: configurationAlarm Package: server.MemoryThresholdCrossingAlarm Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: lowMemoryConfigured	Release: • N/A
Description: The alarm is raised when the available memory on the 5620 SAM server drops below the warning threshold.		
Remedial action: Informational - Memory threshold settings are not configurable. Please contact your Nokia support representative for assistance.		

Table 39-538 MFibTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: MFibTableSizeLimitReached (190) Type: resourceAlarm Package: vpls.MFibTableSizeLimitReached Raised on classes: • vpls.AbstractBSite • vpls.AbstractTlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives a svcTlsMfibTableFullAlarmRaised trap for a VPLS site. The alarm clears when the 5620 SAM receives a svcTlsMfibTableFullAlarmCleared trap for the site.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why		

Table 39-539 MGMCSwitchOverStatusNotify

Alarm	Attributes	Applicable major release
Name: MGMCSwitchOverStatusNotify (4814) Type: processingErrorAlarm Package: multichassis.MGMCSwitchOverStatusNotify Raised on class: multichassis.MultiChassisPeerMobileGateway	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The alarm is raised when the status of switchover enforced on the mobile-gateway in geo-redundancy changes		
Remedial action: Check switchover failure reason and correct the issue in order to perform switchover.		

Table 39-540 MgwPeerGtpMismatchAlarm

Alarm	Attributes	Applicable major release
Name: MgwPeerGtpMismatchAlarm (5144) Type: configurationAlarm Package: wlangw.MgwPeerGtpMismatchAlarm Raised on class: wlangw.MgwPeer	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MgwPeerGtpMismatchAlarm	Release: • N/A
Description: This alarm is raised when the Negotiated QoS profile RADIUS attribute contains a release indicator either for GGSN or PGW that does not correspond to the interface type actually used in GTP. e.g. the release indicator is for GGSN and the interface type used in GTP is S2a/S2b while it should be Gn.		
Remedial action: The RADIUS Server configuration should be corrected to match the MgwPeer interface type actually used in GTP.		

Table 39-541 MicroBFDSessionDown

Alarm	Attributes	Applicable major release
Name: MicroBFDSessionDown (4997) Type: lnkaggAlarm Package: lag.MicroBFDSessionDown Raised on class: lag.Interface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LagMemberMicroBfdSession-StateChanged	Release: • N/A
Description: The alarm is raised when there is a change in the state of the micro-BFD session of a link (port) of the LAG. When the state is 'idle', 'failed', 'waitingFwd', 'up', then the port is forwarding traffic. When the state is 'waiting', 'down', then the port is not forwarding traffic.		
Remedial action: Micro BFD Session state of one of the LAG links is changed. Please check the LAG's BFD configuration or the configuration of the LAG and the Ports in it.		

Table 39-542 MidLevelIPv6RoutesReached

Alarm	Attributes	Applicable major release
Name: MidLevelIPv6RoutesReached (506) Type: ProtocolAlarm Package: l3fwd.MidLevelIPv6RoutesReached Raised on class: l3fwd.ServiceSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MidLevelIPv6RoutesReached	Release: • N/A
Description: The alarm is raised when the number of IPv6 routes in a VPRN exceeds the configured threshold value. The alarm information includes the number of IPv6 routes and the threshold value.		
Remedial action: The number of IPv6 routes has exceeded the configured maximum for the VPRN - the route table must be examined to ensure that all of the routes in the table are valid and not the result of a misconfiguration in the VPRN service. If all of the routes appear to be valid then the value used as the threshold value should be revisited.		

Table 39-543 MidLevelRoutesReached

Alarm	Attributes	Applicable major release
Name: MidLevelRoutesReached (1199) Type: ProtocolAlarm Package: l3fwd.MidLevelRoutesReached Raised on class: l3fwd.ServiceSite	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MidLevelRoutesReached	Release: • N/A
Description: The alarm is raised when the number of routes in a VPRN exceeds the threshold specified in the VPRN configuration. The threshold value is a percentage of the maximum number of routes specified in the VPRN configuration. The alarm information includes the number of routes and the threshold value.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE or VRF instance in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-544 MirrorDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: MirrorDestinationMisconfigured (209) Type: configurationAlarm Package: mirror.MirrorDestinationMisconfigured Raised on class: mirror.Mirror	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mirrorDestinationMisconfig-ured	Release: • N/A
Description: The alarm is raised when more than two destination Sites are configured for a service mirror.		
Raising condition: ('destinationMisconfigured' EQUAL 'true')		
Clearing condition: ('destinationMisconfigured' EQUAL 'false')		
Remedial action: Delete destination site so that there are two or less destination sites in one Mirror service.		

Table 39-545 MirrorEncapsulationTypeInconsistent

Alarm	Attributes	Applicable major release
Name: MirrorEncapsulationTypeInconsistent (217) Type: configurationAlarm Package: mirror.MirrorEncapsulationTypeInconsistent Raised on class: mirror.Mirror	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mirrorEncapsulationTypeIn-consistent	Release: • N/A
Description: The alarm is raised when the encapsulation types of the mirror sites differ.		
Raising condition: ('encapsulationTypeInconsistent' EQUAL 'true')		
Clearing condition: ('encapsulationTypeInconsistent' EQUAL 'false')		
Remedial action: Reconfigure the 'Encapsulation Type' for the sites (delete and re-add the sites if not configurable) so that the 'Encapsulation Type' are the same in one Mirror service.		

Table 39-546 MisconfiguredNode

Alarm	Attributes	Applicable major release
Name: MisconfiguredNode (382) Type: configurationAlarm Package: netw.MisconfiguredNode Raised on class: netw.Topology	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: persistOff Applicable probable causes: • persistOff • noSystemAddress • noIpv4Address • duplicateSystemAddress • sameManagementSystemAddress • noAdminDomainFound • sysIdentifierFail • duplicatedNodeName	Release: • N/A
Description: The alarm is raised when the 5620 SAM tries to discover an NE that is not properly configured for management. For example, when persistence is set to Off in the NE BOF, when the NE has no system address or NE share same management and system address.		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 39-547 mismatchAnyCastRPTypes

Alarm	Attributes	Applicable major release
Name: mismatchAnyCastRPTypes (270) Type: configurationAlarm Package: pim.mismatchAnyCastRPTypes Raised on class: pim.AnyCastRP	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mismatchAnyCastRPTypes	Release: • N/A
Description: The alarm is raised when there is an anycast RP type mismatch.		
Remedial action: A configuration error has occurred that must be corrected. Please check to make sure the global Virtual Anycast RP service type and this PIM Anycast RP service type are consistent.		

Table 39-548 mismatchBackupAddress

Alarm	Attributes	Applicable major release
Name: mismatchBackupAddress (279) Type: configurationAlarm Package: vrrp.mismatchBackupAddress Raised on class: vrrp.VRInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mismatchBackupAddress	Release: • N/A
Description: The alarm is raised when two VR instances in a VR have different backup addresses.		
Remedial action: Reconfigure the backup addresses for the peer VRRP instances so that they are the same.		

Table 39-549 mismatchSubnets

Alarm	Attributes	Applicable major release
Name: mismatchSubnets (280) Type: configurationAlarm Package: vrrp.mismatchSubnets Raised on class: vrrp.VRInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchSubnets	Release: • N/A
Description: The alarm is raised when two VR Instances in a VR have backup addresses that are in different subnets.		
Remedial action: Reconfigure the ip addresses for the peer VRRP instances so that they are in the same subnets.		

Table 39-550 mismatchVrrpTypes

Alarm	Attributes	Applicable major release
Name: mismatchVrrpTypes (278) Type: configurationAlarm Package: vrrp.mismatchVrrpTypes Raised on class: vrrp.VRInstance	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchVrrpTypes	Release: • N/A
Description: The alarm is raised when two VR instances in a VR are of different types, for example, when one VR instance type is Network and the other is IES.		

Table 39-550 mismatchVrrpTypes (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('VRRP Type' NOT EQUAL 'VRRP Type'))		
Clearing condition: (('VRRP Type' EQUAL 'VRRP Type'))		
Remedial action: Reconfigure the VRRP instance peers so that they are from the same type of interfaces (Network, IES or VPRN).		

Table 39-551 MissedStatsCatchUpCollection

Alarm	Attributes	Applicable major release
Name: MissedStatsCatchUpCollection (2895) Type: communicationsAlarm Package: netw.MissedStatsCatchUpCollection Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: snmpDown	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with the node to retrieve missed collections intervals. It is cleared after 5620 SAM main server can retrieve missed collections intervals.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM.		

Table 39-552 MissedStatsCollection

Alarm	Attributes	Applicable major release
Name: MissedStatsCollection (355) Type: communicationsAlarm Package: netw.MissedStatsCollection Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server cannot collect statistics from the node during a statistics poll. It is cleared after 5620 SAM main server can collect statistics from the node during a statistics poll.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the node and the SAM server cannot be established.		

Table 39-553 MissingFallingEvent

Alarm	Attributes	Applicable major release
Name: MissingFallingEvent (414) Type: configurationAlarm Package: rmon.MissingFallingEvent Raised on class: rmon.Alarm	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot find the falling event object that is named in an RMON policy alarm definition.		

Table 39-553 MissingFallingEvent (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Missing Falling Event' EQUAL 'true')		
Clearing condition: ('Missing Falling Event' EQUAL 'false')		
Remedial action: Cannot find the falling event object that is named in an RMON policy alarm definition. Please create the required event.		

Table 39-554 MissingHopConfiguration

Alarm	Attributes	Applicable major release
Name: MissingHopConfiguration (350) Type: configurationAlarm Package: mpls.MissingHopConfiguration Raised on class: mpls.StaticLsp	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MissingHopConfiguration	Release: • N/A
Description: The alarm is raised when a static LSP is created without hops.		
Remedial action: Need to configure static hops to the destination.		

Table 39-555 MissingNESelfConfigPolicy

Alarm	Attributes	Applicable major release
Name: MissingNESelfConfigPolicy (1944) Type: communicationsAlarm Package: netw.MissingNESelfConfigPolicy Raised on class: netw.TopologyDiscoveryRule	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: noNESelfConfigPolicyFound	Release: • N/A
Description: The alarm is raised when an identifier of a shadow NE matches the identifier of a node being discovered by a scan of this discovery rule, but there is no NE self-config policy for the node type set in this discovery rule.		
Remedial action: A configuration error has been made which must be corrected. Create a NE self-config policy and assign it to the discovery rule associated with the node being discovered.		

Table 39-556 MissingPreProvisionedNode

Alarm	Attributes	Applicable major release
Name: MissingPreProvisionedNode (1945) Type: communicationsAlarm Package: netw.MissingPreProvisionedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: noPreProvisionedNodeFound	Release: • N/A
Description: The alarm is raised when there is no pre-provisioned NE with which to associate the discovered candidate target NE.		
Remedial action: A configuration error has been made which must be corrected. Create a pre-provisioned NE for the node being discovered.		

Table 39-557 MissingRisingEvent

Alarm	Attributes	Applicable major release
Name: MissingRisingEvent (413) Type: configurationAlarm Package: rmon.MissingRisingEvent Raised on class: rmon.Alarm	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: incompleteConfig	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot find the rising event object that is named in an RMON policy alarm definition.		
Raising condition: ('Missing Rising Event' EQUAL 'true')		
Clearing condition: ('Missing Rising Event' EQUAL 'false')		
Remedial action: Cannot find the rising event object that is named in an RMON policy alarm definition. Please create the required event.		

Table 39-558 missingStaticRPConfigurations

Alarm	Attributes	Applicable major release
Name: missingStaticRPConfigurations (268) Type: configurationAlarm Package: pim.missingStaticRPConfigurations Raised on class: pim.VirtualAnyCastRP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingStaticRPConfigura-tions	Release: • N/A
Description: The alarm is raised when a static RP configuration is missing.		
Remedial action: A configuration error has occurred that must be corrected. Please check the global Virtual Anycast RP configuration and its operational status flag so that the Static RP and Group Range(s) are all configured.		

Table 39-559 MissSpokeConfiguration

Alarm	Attributes	Applicable major release
Name: MissSpokeConfiguration (218) Type: configurationAlarm Package: vpls.MissSpokeConfiguration Raised on class: vpls.AbstractVpls	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missSpokeConfiguration	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a spoke SDP binding between two sites in one M-VPLS or VPLS. The alarm is not raised by the 5620 SAM, Release 4.0 or later.		
Raising condition: ('missSpokeConfiguration' EQUAL 'true')		
Clearing condition: ('missSpokeConfiguration' EQUAL 'false')		
Remedial action: Deprecated since Rel.4.0		

Table 39-560 MldGrpIfSapCModeRxQueryMism

Alarm	Attributes	Applicable major release
Name: MldGrpIfSapCModeRxQueryMism (5390) Type: configurationAlarm Package: mld.MldGrpIfSapCModeRxQueryMism Raised on class: mld.GrpInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidCompatibilityMode-ofQueryReceived	Release: • N/A
Description: The alarm is raised when there is a mismatch between the compatible mode of the MLD SAP and the version of the received query. It is generated when the SAP is in MLDv1 compatible mode but it receives an MLDv2. It will include information on the configured version of the compatibility mode of the SAP, and the version of the received query.		
Remedial action: Change the MLD Version attribute on the MLD Group Interface to match the MLD host version.		

Table 39-561 MldGrpIfSapMaxGroupsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldGrpIfSapMaxGroupsLimitExceeded (5391) Type: configurationAlarm Package: mld.MldGrpIfSapMaxGroupsLimitExceeded Raised on class: mld.GrpInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldGrpIfSapMaxGroupsLimit-Exceeded	Release: • N/A
Description: 'This alarm is raised when an attempt is made to configure a group when the number of groups configured on the SAP, is equal to the 'Maximum Number of Groups' supported on the SAP.'		
Remedial action: Increase the value of the 'Maximum Number of Groups' attribute in the parent MLD group interface so that the number of active MLD groups stays under the configured threshold.		

Table 39-562 MldGrpIfSapMaxGrpSrcLimExcd

Alarm	Attributes	Applicable major release
Name: MldGrpIfSapMaxGrpSrcLimExcd (5392) Type: configurationAlarm Package: mld.MldGrpIfSapMaxGrpSrcLimExcd Raised on class: mld.GrpInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldGrpIfSapMaxGrpSr-cLimExcd	Release: • N/A
Description: This alarm is raised when an attempt is made to configure a group source for a group when the number of group sources is equal to the 'Maximum Number of Group Sources' per group supported on the SAP.		
Remedial action: Increase the value of the 'Maximum Number Of Group Sources' attribute in the parent MLD group interface so that the number of active MLD Group sources stays under the configured threshold.		

Table 39-563 MldGrpIfSapMaxSourcesLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldGrpIfSapMaxSourcesLimitExceeded (5393) Type: configurationAlarm Package: mld.MldGrpIfSapMaxSourcesLimitExceeded Raised on class: mld.GrpInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldGrpIfSapMaxSourcesLimit-Exceeded	Release: • N/A
Description: 'This alarm is raised when an attempt is made to configure a source for a group when the number of sources for this group is equal to the 'Maximum Number of Sources' per group supported on the SAP.'		
Remedial action: Increase the value of the 'Maximum Number Of Sources' attribute in the parent MLD group interface so that the number of active MLD sources stays under the configured threshold.		

Table 39-564 MldGrpIfSapRxQueryVerMism

Alarm	Attributes	Applicable major release
Name: MldGrpIfSapRxQueryVerMism (5394) Type: configurationAlarm Package: mld.MldGrpIfSapRxQueryVerMism Raised on class: mld.GrpInterfaceSap	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidVersionofQueryMes-sageReceived	Release: • N/A
Description: The alarm is raised when the MLD host SAP is configured as MLDv2 but receives an MLDv1 Query. It will include information on the configured version of the SAP, and the version of the received query.		
Remedial action: Change the MLD Version attribute on the MLD Group Interface to match the MLD host version.		

Table 39-565 MldHostCModeRxQueryMismatch

Alarm	Attributes	Applicable major release
Name: MldHostCModeRxQueryMismatch (8051) Type: configurationAlarm Package: mld.MldHostCModeRxQueryMismatch Raised on class: mld.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidCompatibilityMode-OfQueryReceived	Release: • N/A
Description: The alarm is raised when there is a mismatch between the compatible mode of the MLD Host and the version of the received query, i.e. the Host is in MLDv1 compatible mode but it receives a MLDv2 Query.		
Remedial action: Change the MLD Version attribute on the MLD Group Interface to match the MLD host version.		

Table 39-566 MldHostInstantiationFail

Alarm	Attributes	Applicable major release
Name: MldHostInstantiationFail (8052) Type: configurationAlarm Package: mld.MldHostInstantiationFail Raised on class: mld.GrpInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldHostInstantiationFailed	Release: • N/A
Description: This alarm is generated when a host is eligible for running MLD, but MLD cannot be started on the host.		
Remedial action: A host is eligible for running MLD, but MLD cannot be started on the given host.		

Table 39-567 MldHostMaxGroupsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldHostMaxGroupsLimitExceeded (8053) Type: configurationAlarm Package: mld.MldHostMaxGroupsLimitExceeded Raised on class: mld.GrpInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldHostMaxGroupsLimitExceeded	Release: • N/A
Description: This alarm is generated when an attempt is made to configure a group when the number of groups configured on the PIM interface is equal to the maximum number of groups supported on the host.		
Remedial action: Increase the value of the 'Maximum Number of Groups' attribute in the MLD group interface so that the number of active MLD groups stays under the configured threshold.		

Table 39-568 MldHostMaxGrpSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldHostMaxGrpSrcsLimitExceeded (8054) Type: configurationAlarm Package: mld.MldHostMaxGrpSrcsLimitExceeded Raised on class: mld.GrpInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldHostMaxGrpSrcsLimitExceeded	Release: • N/A
Description: The alarm is generated when an attempt is made to configure a source for a group when the number of group sources is equal to the maximum number of group sources per group supported on the host.		
Remedial action: Increase the value of the 'Maximum Number Of Group Sources' attribute in the MLD group interface so that the number of active MLD Group sources stays under the configured threshold.		

Table 39-569 MldHostMaxSrcsLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldHostMaxSrcsLimitExceeded (8055) Type: configurationAlarm Package: mld.MldHostMaxSrcsLimitExceeded Raised on class: mld.GrpInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MldHostMaxSrcsLimitExceeded	Release: • N/A
Description: The alarm is generated when an attempt is made to configure a source for a group when the number of sources for this group is equal to the maximum number of sources per group supported on the host.		
Remedial action: Increase the value of the 'Maximum Number Of Sources' attribute in the MLD group interface so that the number of active MLD sources stays under the configured threshold.		

Table 39-570 MldHostRxQueryVerMismatch

Alarm	Attributes	Applicable major release
Name: MldHostRxQueryVerMismatch (8056) Type: configurationAlarm Package: mld.MldHostRxQueryVerMismatch Raised on class: mld.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidVersionOfQueryMessageReceived	Release: • N/A
Description: The alarm is raised when the MLD host is configured as MLDv2 but receives an MLDv1 Query. It will include information on the configured version of MLD Host, and the version of the received query.		
Remedial action: Change the MLD Version attribute on the MLD Group Interface to match the MLD host version.		

Table 39-571 MldSnpgGrpDroppedLimitExceeded

Alarm	Attributes	Applicable major release
Name: MldSnpgGrpDroppedLimitExceeded (537) Type: AccessInterfaceAlarm Package: vpls.MldSnpgGrpDroppedLimitExceeded Raised on class: vpls.L2AccessInterfaceMldSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: mldSnpgGrpMaxNbrGrpsReached	Release: • N/A
Description: The alarm is raised when a SAP drops an MLD group because the configurable maximum number of MLD groups on the SAP is reached.		
Remedial action: Increasing the maximum number of MLD Groups to prevent groups from being dropped.		

Table 39-572 MlpppBundleInterleavingDisabled

Alarm	Attributes	Applicable major release
Name: MlpppBundleInterleavingDisabled (4383) Type: other Package: netw.MlpppBundleInterleavingDisabled Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mlpppBundleInterleavingDisabled	Release: • N/A
Description: The alarm is raised when the 'Link Fragmentation and LFI' bit is set but LFI isn't active for MLPPP Bundle. It is cleared for other cases. If LFI is not desired, disable it in the L2TP MLPPP configuration of the related routing instance. Or, ensure that the MLPPP bundle only contains a single link.		
Remedial action: If LFI is not desired, disable it in the L2TP MLPPP configuration of the related routing instance. Or, ensure that the MLPPP bundle only contains a single link.		

Table 39-573 MobGwSysGrpWriteCdrToCfAlarm

Alarm	Attributes	Applicable major release
Name: MobGwSysGrpWriteCdrToCfAlarm (3634) Type: MgGroupAlarm Package: isa.MobGwSysGrpWriteCdrToCfAlarm Raised on class: isa.MgIsaGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MobGwSysGrpWriteCdrToCfStop	Release: • N/A
Description: The alarm is raised when the SGW or PGW writes Charging Data Record (CDR) packets to the local compact flash for the mobile system group.		
Remedial action: Retrieve Charging Data Record (CDR) files from compact flash.		

Table 39-574 ModFail

Alarm	Attributes	Applicable major release
Name: ModFail (1171) Type: communicationsAlarm Package: equipment.ModFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: modFail	Release: • N/A
Description: The alarm is raised when a modulation failure is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-575 ModLOS

Alarm	Attributes	Applicable major release
Name: ModLOS (1172) Type: communicationsAlarm Package: equipment.ModLOS Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: modLOS	Release: • N/A
Description: The alarm is raised when a modulation loss of signal is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-576 ModuleOutOfMemory

Alarm	Attributes	Applicable major release
Name: ModuleOutOfMemory (180) Type: equipmentAlarm Package: netw.ModuleOutOfMemory Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: outOfMemory	Release: • N/A
Description: The alarm is raised when the available NE memory is insufficient for allocation to a task.		
Remedial action: Informational - If the alarm persists please contact your Nokia support representative for assistance		

Table 39-577 MonitoredObjectsCrossThreshold

Alarm	Attributes	Applicable major release
Name: MonitoredObjectsCrossThreshold (8146) Type: processingErrorAlarm Package: sup.MonitoredObjectsCrossThreshold Raised on class: sup.SupervisionManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MonitoredObjectsCrossThreshold	Release: • N/A
Description: This alarm is raised when total monitored objects count cross certain threshold. It is in warning when the total count exceeds 90% of the limit, and in critical when the total count reaches the limit. It is automatically cleared when the total count is back under the limit and threshold.		
Remedial action: Please remove unnecessary supervision groups or change the inclusion filters of supervision groups to reduce monitored objects.		

Table 39-578 MplsResignalTimerExpired

Alarm	Attributes	Applicable major release
Name: MplsResignalTimerExpired (1121) Type: ProtocolAlarm Package: mpls.MplsResignalTimerExpired Raised on class: mpls.Site	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resignalTimerExpired	Release: • N/A

Table 39-578 MplsResignalTimerExpired (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an MPLS instance resignal timer expires.		
Remedial action: Informational only.		

Table 39-579 MPTCardFailure

Alarm	Attributes	Applicable major release
Name: MPTCardFailure (4830) Type: equipmentAlarm Package: mwa.MPTCardFailure Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitProblem	Release: • N/A
Description: This alarm is raised when MPT card failure is detected.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-580 MPTPlugInCardFailure

Alarm	Attributes	Applicable major release
Name: MPTPlugInCardFailure (4831) Type: equipmentAlarm Package: mwa.MPTPlugInCardFailure Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitProblem	Release: • N/A
Description: This alarm is raised when RPS/XPIC Plug-in card failure is detected.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-581 MPTPowerSupplyFailure

Alarm	Attributes	Applicable major release
Name: MPTPowerSupplyFailure (1170) Type: equipmentAlarm Package: equipment.MPTPowerSupplyFailure Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • N/A
Description: The alarm is raised when an MPT radio power source has a power supply failure.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-582 msapCreationFailure

Alarm	Attributes	Applicable major release
Name: msapCreationFailure (740) Type: ConfigurationAlarm Package: vpls.msapCreationFailure Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: creationFailure Applicable probable causes: • creationFailure • radiusAuthFailed	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot create an MSAP.		
Remedial action: This warning is raised when the NE fails to create an MSAP.\nPlease review the alarm's additional text to obtain information about the error condition. Possible problems can be mis-configuration of the capture SAP, authentication failures, a missing target service or interface, illegal trigger packets and more.		

Table 39-583 MsdpActSrcLimExcd

Alarm	Attributes	Applicable major release
Name: MsdpActSrcLimExcd (380) Type: communicationsAlarm Package: msdp.MsdpActSrcLimExcd Raised on class: msdp.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MsdpActiveSourcesLimitExceeded	Release: • N/A
Description: The alarm is raised when an MSDP site receives a number of source active messages that exceeds the configured maximum.		
Remedial action: Increase the configurable maximum number of source active messages if possible.		

Table 39-584 MsdpGroupSrcActMsgsExcd

Alarm	Attributes	Applicable major release
Name: MsdpGroupSrcActMsgsExcd (378) Type: communicationsAlarm Package: msdp.MsdpGroupSrcActMsgsExcd Raised on class: msdp.PeerGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MsdpGroupActiveSourcesLimitExceeded	Release: • N/A
Description: The alarm is raised when an MSDP group receives a number of source active messages that exceeds the configured maximum.		
Remedial action: Increase the configurable maximum number of source active messages if possible.		

Table 39-585 MsdpPeerActSrcLimExcd

Alarm	Attributes	Applicable major release
Name: MsdpPeerActSrcLimExcd (379) Type: communicationsAlarm Package: msdp.MsdpPeerActSrcLimExcd Raised on classes: • msdp.Peer • msdp.GroupPeer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MsdpPeerActiveSourcesLimit-Exceeded	Release: • N/A
Description: The alarm is raised when an MSDP peer receives a number of source active messages that exceeds the configured maximum.		
Remedial action: Increase the configurable maximum number of source active messages if possible.		

Table 39-586 MsdpRPFFailure

Alarm	Attributes	Applicable major release
Name: MsdpRPFFailure (354) Type: communicationsAlarm Package: msdp.MsdpRPFFailure Raised on class: msdp.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MsdpRPFFailure	Release: • N/A
Description: The alarm is raised when an MSDP site experiences an RPF failure.		
Remedial action: Informational.		

Table 39-587 MsdpSourceSrcActMsgsExcd

Alarm	Attributes	Applicable major release
Name: MsdpSourceSrcActMsgsExcd (381) Type: communicationsAlarm Package: msdp.MsdpSourceSrcActMsgsExcd Raised on class: msdp.Source	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MsdpSourceActive-SourcesLimitExceeded	Release: • N/A
Description: The alarm is raised when an MSDP source receives a number of source active messages that exceeds the configured maximum.		
Remedial action: Increase the configurable maximum number of source active messages if possible.		

Table 39-588 MsPwFecMisConfig

Alarm	Attributes	Applicable major release
Name: MsPwFecMisConfig (3691) Type: serviceAlarm Package: svt.MsPwFecMisConfig Raised on class: svt.SpokeSdpFec	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: msPwFecMisConfig	Release: • N/A
Description: The alarm is raised when a misconfiguration is discovered between two signaling multi-segment pseudowires. For example, configuring both multi-segment pseudowires as master would cause this notification.		
Clearing condition: ('Administrative State' EQUAL 'Up')		
Remedial action: Configure multi-segment pseudo-wires such that both are not configured to be master.		

Table 39-589 MultiChassisStpBlockingStatus

Alarm	Attributes	Applicable major release
Name: MultiChassisStpBlockingStatus (4902) Type: communicationsAlarm Package: aosredundancy. MultiChassisStpBlockingStatus Raised on class: aosredundancy.AOSMultiChassis	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PrimarybridgeSTPPriority-ishigherthansecondrybridge	Release: • N/A
Description: Primary bridge STP Priority is higher than secondary bridge		
Remedial action: This Alarm can be cleared by setting primary bridge STP Priority lower then secondary bridge stp priority		

Table 39-590 MultipleOwners

Alarm	Attributes	Applicable major release
Name: MultipleOwners (283) Type: configurationAlarm Package: vrrp.MultipleOwners Raised on class: vrrp.AbstractInstance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: multipleOwnersConfigured	Release: • N/A
Description: The alarm is raised when an owner VR instance detects another instance that advertises itself as an owner.		
Remedial action: Shut down one of the peer VRRP instances and change the owner to false and then turn it up.		

Table 39-591 multipleRPLOwner

Alarm	Attributes	Applicable major release
Name: multipleRPLOwner (2946) Type: configurationAlarm Package: ethring.multipleRPLOwner Raised on class: ethring.Element	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: multiplerpl	Release: • N/A

Table 39-591 multipleRPLOwner (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised on RPL elements configured as RPL owners, when there are multiple RPL owners detected in the ring topology.		
Remedial action: A configuration error has been made which must be corrected. The duplicate RPL owners must be deleted.		

Table 39-592 MVPNDuplicateVrfPolicy

Alarm	Attributes	Applicable major release
Name: MVPNDuplicateVrfPolicy (649) Type: configurationAlarm Package: l3fwd.MVPNDuplicateVrfPolicy Raised on classes: • l3fwd.ServiceSiteMVPNImportPolicy • l3fwd.ServiceSiteMVPNExportPolicy	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: duplicateVrfPolicyExists	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a duplicate VRF policy in a multicast VPRN. The alarm information includes the VRF policy ID and type, and information about the service site. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has occurred which must be corrected. The duplicate VRF policy must be removed. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-593 MVPNExportPolicyNotFound

Alarm	Attributes	Applicable major release
Name: MVPNExportPolicyNotFound (650) Type: configurationAlarm Package: l3fwd.MVPNExportPolicyNotFound Raised on class: l3fwd.ServiceSiteMVPNExportPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: exportPolicyDoesNotExist	Release: • N/A
Description: The alarm is raised when a VRF export policy for a multicast VPRN cannot be found. The alarm information includes the policy ID. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has occurred which must be corrected. A VRF export policy with the appropriate ID must be configured. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-594 MVPNImportPolicyNotFound

Alarm	Attributes	Applicable major release
Name: MVPNImportPolicyNotFound (651) Type: configurationAlarm Package: l3fwd.MVPNImportPolicyNotFound Raised on class: l3fwd.ServiceSiteMVPNImportPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: importPolicyDoesNotExist	Release: • N/A

Table 39-594 MVPNImportPolicyNotFound (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a VRF import policy for a multicast VPRN cannot be found. The alarm information includes the policy ID. Note: starting from SAM 12.0 R1, SAM no longer raise this alarm since it is not much useful but has performance issue.		
Remedial action: A configuration error has occurred which must be corrected. A VRF import policy with the appropriate ID must be configured. Note: starting from SAM 12.0 R1, SAM no longer raises this alarm.		

Table 39-595 MwLinkEPSActivityChange

Alarm	Attributes	Applicable major release
Name: MwLinkEPSActivityChange (4945) Type: communicationsAlarm Package: mwa.MwLinkEPSActivityChange Raised on class: mwa.MwLink	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: EPSActivityChange	Release: • N/A
Description: This alarm is raised when a microwave link changes activity for EPS.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-596 MwLinkMaintenanceChange

Alarm	Attributes	Applicable major release
Name: MwLinkMaintenanceChange (4946) Type: communicationsAlarm Package: mwa.MwLinkMaintenanceChange Raised on class: mwa.MwLink	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: MaintenanceCommand-Change	Release: • N/A
Description: This alarm is raised when a microwave link maintenance command changes.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-597 MwLinkPeerChange

Alarm	Attributes	Applicable major release
Name: MwLinkPeerChange (4832) Type: communicationsAlarm Package: mwa.MwLinkPeerChange Raised on class: mwa.MwLink	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PeerChange	Release: • N/A
Description: This alarm is raised when a microwave link discovered peer changes.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-598 MwLinkRPSActivityChange

Alarm	Attributes	Applicable major release
Name: MwLinkRPSActivityChange (4947) Type: communicationsAlarm Package: mwa.MwLinkRPSActivityChange Raised on class: mwa.MwLink	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: RPSActivityChange	Release: • N/A
Description: This alarm is raised when a microwave link changes activity for RPS.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-599 MwLinkTPSActivityChange

Alarm	Attributes	Applicable major release
Name: MwLinkTPSActivityChange (4948) Type: communicationsAlarm Package: mwa.MwLinkTPSActivityChange Raised on class: mwa.MwLink	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: TPSActivityChange	Release: • N/A
Description: This alarm is raised when a microwave link changes activity for TPS.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-600 NEBackupRecoveryFailed

Alarm	Attributes	Applicable major release
Name: NEBackupRecoveryFailed (8418) Type: processingErrorAlarm Package: sw.NEBackupRecoveryFailed Raised on class: sw.BackupRestoreManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileError	Release: • N/A
Description: The alarm is raised when an unexpected directory was found during NE backup recovery. The alarm is cleared when all NE backups located on the file system are already in the 5620 SAM database or they are recovered successfully in the 5620 SAM database.		
Remedial action: An NE backup located on the file system could not be imported in the 5620 SAM database. Ensure the directory structure containing the backups has the correct permissions and the directory names are properly formatted.		

Table 39-601 NeDatafileSizeAboveThreshold

Alarm	Attributes	Applicable major release
Name: NeDatafileSizeAboveThreshold (4975) Type: databaseAlarm Package: db.NeDatafileSizeAboveThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: HighNumberOfRecords	Release: • N/A

Table 39-601 NeDatafileSizeAboveThreshold (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a tablespace data file size exceeds the used space threshold. This may indicate that the number of stored NE backups or software images is too high.		
Remedial action: The probable cause of this alarm is the storage of too many NE backup or software image files. Purge old backup or extra software image files from the SAM database to resolve the problem. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-602 NeighborEntriesExceededLimit (rtr)

Alarm	Attributes	Applicable major release
Name: NeighborEntriesExceededLimit (9590) Type: communicationsAlarm Package: rtr.NeighborEntriesExceededLimit Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NeighborEntriesExceeded-Limit	Release: • N/A
Description: The alarm is raised when the maximum amount of IPv6 neighbor entries learned on an IP interface has exceeded the configured maximum.		
Remedial action: Need to increase the Neighbor limit since number of IPv6 Neighbor entries have exceeded the configured limit so no new entries are learned until an entry expires.		

Table 39-603 NeighborEntriesExceededLimit (service)

Alarm	Attributes	Applicable major release
Name: NeighborEntriesExceededLimit (9590) Type: communicationsAlarm Package: service.NeighborEntriesExceededLimit Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NeighborEntriesExceeded-Limit	Release: • N/A
Description: The alarm is raised when the maximum amount of IPv6 neighbor entries learned on an IP interface has exceeded the configured maximum.		
Remedial action: Need to increase the Neighbor limit since number of IPv6 Neighbor entries have exceeded the configured limit so no new entries are learned until an entry expires.		

Table 39-604 NeighborEntriesExceededThresholdLimit (service)

Alarm	Attributes	Applicable major release
Name: NeighborEntriesExceededThresholdLimit (9591) Type: communicationsAlarm Package: service. NeighborEntriesExceededThresholdLimit Raised on class: service.L3AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NeighborEntriesExceed-edThresholdLimit	Release: • N/A
Description: The alarm is raised when the number of IPv6 neighbor entries learned on an IP interface has exceeded vRtrIfIpv6NbrThreshold percent of the configured maximum as specified by vRtrIfIpv6NbrLimit.		
Remedial action: Need to increase the Neighbor limit.		

Table 39-605 NeighborEntriesExceededThresholdLimit (rtr)

Alarm	Attributes	Applicable major release
Name: NeighborEntriesExceededThresholdLimit (9591) Type: communicationsAlarm Package: rtr.NeighborEntriesExceededThresholdLimit Raised on class: rtr.NetworkInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NeighborEntriesExceed-edThresholdLimit	Release: • N/A
Description: The alarm is raised when the number of IPv6 neighbor entries learned on an IP interface has exceeded vRtrIfIpv6NbrThreshold percent of the configured maximum as specified by vRtrIfIpv6NbrLimit.		
Remedial action: Need to increase the Neighbor limit.		

Table 39-606 NeighborLoss (pim)

Alarm	Attributes	Applicable major release
Name: NeighborLoss (188) Type: communicationsAlarm Package: pim.NeighborLoss Raised on class: pim.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborConnectionLost	Release: • N/A
Description: The alarm is raised when the connection to a neighbor is lost.		
Remedial action: Informational - please check the connection to the neighbor is fine, e.g the peer is not in shutdown state. The alarm will be cleared when the neighbor is discovered up.		

Table 39-607 NeighborLoss (vpls)

Alarm	Attributes	Applicable major release
Name: NeighborLoss (188) Type: communicationsAlarm Package: vpls.NeighborLoss Raised on class: vpls.InterfacePimSnooping	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborConnectionLost	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a loss of connection to a PIM neighbor.		
Remedial action: There is a lost connection to the PIM Neighbor. Check the PIM Neighbor to ensure it is still operational and that underlying transport of the SAP or SDP is operationally up.		

Table 39-608 NetConfEventSubscriptionProblem

Alarm	Attributes	Applicable major release
Name: NetConfEventSubscriptionProblem (4864) Type: communicationsAlarm Package: netw.NetConfEventSubscriptionProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NetConfEventSubscription-Failed	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to subscribe for Netconf event notification from a network element. For a WMM or CMM: if this problem persists it may result in a loss of PM file collection.		
Remedial action: Informational -if the alarm persists or is occurring frequently then investigation is required to understand why the Netconf event subscription configuration is failing.		

Table 39-609 NetworkElementChassisTypeMismatch

Alarm	Attributes	Applicable major release
Name: NetworkElementChassisTypeMismatch (1946) Type: communicationsAlarm Package: netw.NetworkElementChassisTypeMismatch Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchOfNetworkElement-ChassisType	Release: • N/A
Description: The alarm is raised when the chassis type of the shadow network element does not match with the chassis type of the discovered NE.		
Remedial action: A configuration error has been made which must be corrected. The pre-provisioned NE chassis type defined must match the chassis type of the node being discovered.		

Table 39-610 NetworkElementTypeMismatch

Alarm	Attributes	Applicable major release
Name: NetworkElementTypeMismatch (1947) Type: communicationsAlarm Package: netw.NetworkElementTypeMismatch Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchOfNetworkElement-Type	Release: • N/A
Description: The alarm is raised when the type of the shadow network element does not match with the type of the discovered NE.		
Remedial action: A configuration error has been made which must be corrected. The pre-provisioned NE type defined must match the type of the node being discovered.		

Table 39-611 NetworkElementVersionMismatch

Alarm	Attributes	Applicable major release
Name: NetworkElementVersionMismatch (1948) Type: communicationsAlarm Package: netw.NetworkElementVersionMismatch Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchOfNetworkElement-Version	Release: • N/A
Description: The alarm is raised when the version of the shadow network element does not match with the version of the discovered NE.		
Remedial action: A configuration error has been made which must be corrected. The pre-provisioned NE version defined must match the version of the node being discovered.		

Table 39-612 NodeAlreadyManagedOverAnotherProtocol

Alarm	Attributes	Applicable major release
Name: NodeAlreadyManagedOverAnotherProtocol (1080) Type: discoveryControlAlarm Package: netw. NodeAlreadyManagedOverAnotherProtocol Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeAlreadyDiscovered	Release: • N/A
Description: The alarm is raised when the 5620 SAM tries to rediscover a previously discovered NE using a different IP version.		
Remedial action: Informational		

Table 39-613 NodeColdStart

Alarm	Attributes	Applicable major release
Name: NodeColdStart (172) Type: equipmentAlarm Package: netw.NodeColdStart Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeColdStart	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives a SNMPv2-MIB.coldStart trap from an NE.		
Remedial action: Informational - 5620 SAM has received an indication from an NE that it has restarted. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-614 NodeDatabaseCorruptionDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseCorruptionDetected (1961) Type: communicationsAlarm Package: netw.NodeDatabaseCorruptionDetected Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseCorrupted	Release: • N/A
Description: This alarm is raised when an error in the node causes the node to lose its configuration and come up in an inconsistent/incomplete state. To overcome this it might be necessary to reconfigure the node.		
Remedial action: The node configuration is inconsistent. You may have to do a Reconfigure. However if it's a first discovery, you have to delete the node, then create a pre-provisioned NE instance, create a new discovery rule with a self-configuration policy and discover the node.		

Table 39-615 NodeDataMismatch

Alarm	Attributes	Applicable major release
Name: NodeDataMismatch (3315) Type: configurationAlarm Package: netw.NodeDataMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: nodeDataMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM Data model and node is mismatched.		
Remedial action: Resync the object or update it with the appropriate values.		

Table 39-616 NodeSoftwareMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeSoftwareMisalignmentDetected (4906) Type: communicationsAlarm Package: netw.NodeSoftwareMisalignmentDetected Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeSoftwareMisalignment	Release: • N/A

Table 39-616 NodeSoftwareMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a software misalignment has been detected on the node and comes back up with an unexpected software version (software change triggered by external tool) To correct this situation it is necessary to download and activate on the node the software referenced by SAM and then reconfigure the node with the 5620 SAM's current configuration.		
Remedial action: the NE software is misaligned. Perform a Download and Activate Software operation with the software version known by SAM which is the reference.		

Table 39-617 NodeUpgraded

Alarm	Attributes	Applicable major release
Name: NodeUpgraded (178) Type: configurationAlarm Package: netw.NodeUpgraded Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: upgradedNodeVersion	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects an NE software version upgrade.		
Remedial action: Informational		

Table 39-618 NodeVersionMismatch

Alarm	Attributes	Applicable major release
Name: NodeVersionMismatch (177) Type: configurationAlarm Package: netw.NodeVersionMismatch Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DowngradedNodeVersion	Release: • N/A
Description: The alarm is raised when the software version on an NE differs from the version recorded for the NE in the 5620 SAM database.		
Remedial action: The NE has been manually downloaded with a new version of SW. Unmanage and re-manage this node to clear the alarm. If software version on the NE is incompatible with the version of 5620 SAM, then the SW should be reverted to a compatible version for SAM (then unmanage and re-manage the node).		

Table 39-619 NominalLinkViolation

Alarm	Attributes	Applicable major release
Name: NominalLinkViolation (9012) Type: communicationsAlarm Package: gmpls.NominalLinkViolation Raised on class: gmpls.OpticalGLSP	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NominalLinkViolation	Release: • N/A
Description: The alarm is raised for a tunnel LSP on nominal path when at least one tunnel is not on nominal path.		
Remedial action: Not Available.		

Table 39-620 NoRPLOwner

Alarm	Attributes	Applicable major release
Name: NoRPLOwner (3700) Type: configurationAlarm Package: ethring.NoRPLOwner Raised on class: ethring.RadioRing	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: norpltype	Release: • N/A
Description: The alarm is raised when there is No RPL Owner selected on a Radio Ring.		
Remedial action: Operator has to configure at least one of the Elements belonging to a Radio Ring as RPL Owner.		

Table 39-621 NotEnoughContiguousBlocks

Alarm	Attributes	Applicable major release
Name: NotEnoughContiguousBlocks (4987) Type: configurationAlarm Package: dhcp.NotEnoughContiguousBlocks Raised on class: dhcp.LocalDhcp6Server	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: notEnoughContiguousBlocks	Release: • N/A
Description: The alarm is raised when a lease cannot be created because not enough contiguous blocks are found for the requested delegated prefix size.		
Remedial action: This alarm is raised when a lease cannot be created because not enough contiguous blocks are found for the requested delegated prefix size.\n Please adjust the associated pools.		

Table 39-622 NsgVirtualSwitchDown

Alarm	Attributes	Applicable major release
Name: NsgVirtualSwitchDown (11060) Type: virtualSwitchAlarm Package: dctr.NsgVirtualSwitchDown Raised on class: dctr.NsgVirtualSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NsgUplinksAllDown	Release: • N/A
Description: The alarm is raised when all Uplinks of the NSG are down.		
Remedial action: This alarm is raised when all uplinks associated to the NSG are lost.		

Table 39-623 NsgVirtualSwitchPartiallyDown

Alarm	Attributes	Applicable major release
Name: NsgVirtualSwitchPartiallyDown (11061) Type: virtualSwitchAlarm Package: dctr.NsgVirtualSwitchPartiallyDown Raised on class: dctr.NsgVirtualSwitch	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NsgUplinkDown	Release: • N/A
Description: The alarm is raised when some Uplinks of the NSG are down.		

Table 39-623 NsgVirtualSwitchPartiallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when an uplink of the NSG is lost but at least one uplink remains.		

Table 39-624 NTPMaxAssocTrap

Alarm	Attributes	Applicable major release
Name: NTPMaxAssocTrap (9633) Type: communicationsAlarm Package: ntp.NTPMaxAssocTrap Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NTPMaxAssocTrap	Release: • N/A
Description: Notify the management entity on reaching the maximum allowable NTP client and peer associations.		
Remedial action: This is informational alarm to indicate management entity on reaching the maximum allowable NTP client and peer associations.		

Table 39-625 NTPNoServersAvail

Alarm	Attributes	Applicable major release
Name: NTPNoServersAvail (4878) Type: communicationsAlarm Package: ntp.NTPNoServersAvail Raised on class: ntp.NTP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPNoServersAvail	Release: • N/A
Description: The alarm is generated when no NTP Servers are available.		
Remedial action: Please check if the configured servers are physically reachable (IP ping) from the node (Or) check if the configured servers are enabled as NTP Server (NTP Server attribute on General Tab) and their Operational state is Up (Or) check if the authentication keys are correctly defined on the client and the NTP server node.		

Table 39-626 NTPServerChange

Alarm	Attributes	Applicable major release
Name: NTPServerChange (4880) Type: communicationsAlarm Package: ntp.NTPServerChange Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: NTPServerChange	Release: • N/A
Description: The alarm generated when more than one NTP servers are configured in a system and a different NTP server is selected because the operational status of the earlier NTP server has changed.		
Remedial action: This is informational alarm to indicate that the current clock source has changed for the node. Alarm needs to be manually cleared.		

Table 39-627 OAM_120

Alarm	Attributes	Applicable major release
Name: OAM_120 (6153) Type: communicationsAlarm Package: femto.OAM_120 Raised on class: femto.FGW	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • N/A
Description: Loss of OAM link between SAM and FGW.		
Remedial action: No particular action is required. This notification may be required by Global Product Support for debugging purposes		

Table 39-628 OAM_121

Alarm	Attributes	Applicable major release
Name: OAM_121 (6154) Type: communicationsAlarm Package: femto.OAM_121 Raised on class: femto.FGW	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: communicationsSubsystem-Failure	Release: • N/A
Description: The OAMLinkAdministrativeState parameter (FGW object) is equal to locked.		
Remedial action: Find out why the OAMLinkAdministrativeState was locked in the first place. Set the OAMLinkAdministrativeState parameter (FGW object) to unlocked.		

Table 39-629 OAM_122

Alarm	Attributes	Applicable major release
Name: OAM_122 (6155) Type: processingErrorAlarm Package: femto.OAM_122 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The MIB number received from NE is different from the MIB number stored in the active view.		
Remedial action: See the nodal documentation for more information.		

Table 39-630 OAM_123

Alarm	Attributes	Applicable major release
Name: OAM_123 (6156) Type: processingErrorAlarm Package: femto.OAM_123 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The FGW ID received from NE is different from the data configured at SAM.		
Remedial action: Undeclare and then declare the FGW with the correct FGW ID		

Table 39-631 OAM_124

Alarm	Attributes	Applicable major release
Name: OAM_124 (6157) Type: processingErrorAlarm Package: femto.OAM_124 Raised on class: femto.FGW	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: The FGW Cluster ID received from NE is different from the data configured at SAM.		
Remedial action: Undeclare and then declare the FGW with the correct FGW Cluster ID		

Table 39-632 OCHTrailDown

Alarm	Attributes	Applicable major release
Name: OCHTrailDown (3891) Type: communicationsAlarm Package: optical.OCHTrailDown Raised on class: optical.OCHTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the OCH trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-633 OCHTrailMisConfigured

Alarm	Attributes	Applicable major release
Name: OCHTrailMisConfigured (5125) Type: communicationsAlarm Package: optical.OCHTrailMisConfigured Raised on class: optical.OCHTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OchCrossConnectionTrail-NameMisMatch	Release: • N/A

Table 39-633 OCHTrailMisConfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when all the OCh cross connections (XCs) of an OCh trail do not have the same trail name. In order for the auto wavekey processing to work properly, the XC name should be the same on all NEs of the OCh trail.		
Remedial action: Recreate the OCH Cross Connects with same OCH Trail name else Wave Tracker does not work properly.		

Table 39-634 ODUTrailDown

Alarm	Attributes	Applicable major release
Name: ODUTrailDown (3892) Type: communicationsAlarm Package: optical.ODUTrailDown Raised on class: optical.ODUTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the ODU trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-635 ODUTrailMisConfigured

Alarm	Attributes	Applicable major release
Name: ODUTrailMisConfigured (3893) Type: communicationsAlarm Package: optical.ODUTrailMisConfigured Raised on class: optical.ODUTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OchCrossConnectionTrail-NameMisMatch	Release: • N/A
Description: The alarm is raised when all the OCh cross connections (XCs) of an OCh trail do not have the same trail name. In order for the auto wavekey processing to work properly, the XC name should be the same on all NEs of the OCh trail.		
Remedial action: Recreate the OCH Cross Connects with same OCH Trail name else Wave Tracker does not work properly.		

Table 39-636 oesCfgBlocked

Alarm	Attributes	Applicable major release
Name: oesCfgBlocked (11180) Type: equipmentAlarm Package: netw.oesCfgBlocked Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OesConfigurationisNotinSyn-cWithRouter	Release: • N/A
Description: CAUSE This alarm is generated when a configuration being made in the OES was blocked. EFFECT The configuration is not active in the OES.		

Table 39-636 oesCfgBlocked (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1.If there is a card present in the OES and is a supported card type but the router is not yet aware of its presence.This will be cleared as soon as the router becomes aware of the card.\n 2. If the mounted card is supported card and is misaligned with the configuration, move the card to the correct slot.\n 3. If there is an unsupported card type in the OES that the router cannot manage.The OES has to be re-commissioned to clear the condition.		

Table 39-637 oesCfgFailNoMemory

Alarm	Attributes	Applicable major release
Name: oesCfgFailNoMemory (11181) Type: equipmentAlarm Package: netw.oesCfgFailNoMemory Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: requestForDynamicMemoryToDownloadConfigFailed	Release: • N/A
Description: [CAUSE] The oesCfgFailNoMemory notification is generated when a request to obtain dynamic memory to download a configuration to the OES has failed. [EFFECT] The configuration is not active in the OES.		
Remedial action: This may be a temporary issue and the condition may clear on its own. If the event is raised periodically, then there is a permanent memory issue and the support organization should be informed.		

Table 39-638 OesControlCommunicationDown

Alarm	Attributes	Applicable major release
Name: OesControlCommunicationDown (9576) Type: equipmentAlarm Package: netw.OesControlCommunicationDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesControlPathCommunicationDown	Release: • N/A
Description: This alarm generated when the active CPM of SR Chassis can not reach the OES master chassis.		
Remedial action: The Control Path Communication from the router to the OES Master Chassis has gone down. The OES can not be managed by the router. Ensure that all control communications ports between the router and the OES master chassis are correctly connected and test the cables.		

Table 39-639 OesCtlCardPortDown

Alarm	Attributes	Applicable major release
Name: OesCtlCardPortDown (9043) Type: equipmentAlarm Package: equipment.OesCtlCardPortDown Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesCtlCardPortDown	Release: • N/A
Description: This alarm is generated when a port (e.g. ES 1 or AUX) on an OES Control Card is not operational.		

Table 39-639 OesCtlCardPortDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The port on OES control card may be misconnected, disconnected, faulty or having faulty cable or faulty Control card. Check that the cable is correctly connected and test the cable.		

Table 39-640 OesDbInvalid

Alarm	Attributes	Applicable major release
Name: OesDbInvalid (9577) Type: equipmentAlarm Package: equipment.OesDbInvalid Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DbInvalid	Release: • N/A
Description: During installation,if the OES is not properly commissioned. A downgrade of OES software has occurred. A serial number in the database does not match that of the OES either because the controller was replaced or the alarm card was replaced. Equipment Controller is removed/reseated during a system process, causing file corruption. The database audit failed indicating some type of corruption of the database.		
Remedial action: OES database corruption has occured.Recommision the OES to SR shelf. The correct database is held in the host system so it will be restored to the shelf once the existing database is cleared and the host re-establishes communication with the OES.		

Table 39-641 OesDbSyncFailure

Alarm	Attributes	Applicable major release
Name: OesDbSyncFailure (9578) Type: equipmentAlarm Package: equipment.OesDbSyncFailure Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesEquipmentControllerFail-ure	Release: • N/A
Description: This alarm is generated when an active Equipment Controller of OES is unable to synchronize its database with the inactive Equipment Controller. This could be because of incorrectly seated Equipment Controller or the software versions on the active and inactive Equipment Controllers are not compatible or A hardware problem with one or both controllers.		
Remedial action: The OES does not have redundancy protection between the two Equipment Controller cards. \n 1.Remove the Equipment Controller with the condition and examine the connector on the back of the card for damage, including bent or broken pins; \n 2.Examine the connector on the backplane for damage. If there is damage to the backplane of the shelf, contact your service representative; \n 3.Re-insert the Equipment Controller into its original slot and allow the card to initialize; \n 4.Repeat the steps 2 to 3 for the second Equipment Controller. \n 5.Replace the Equipment Controller with the alarm condition with a new unit. If the condition is not cleared, replace the second Equipment Controller with a new unit. Follow the return and repair process to return the faulty card to an authorized repair center for replacement.		

Table 39-642 OesDbUnsync

Alarm	Attributes	Applicable major release
Name: OesDbUnsync (9579) Type: equipmentAlarm Package: equipment.OesDbUnsync Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesEquipmentControllerRedundancySyncFailure	Release: • N/A
Description: This alarm is generated when the active and standby Equipment Controllers are not in sync. This could be because of the OES does not have redundancy protection between the two Equipment Controller cards.		
Remedial action: The OES does not have redundancy protection between the two Equipment Controller cards. If a switchover were to occur, then the database of the newly active controller might not reflect the latest configuration. Perform a warm reset of the standby controller. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-643 OESECSwitchOver

Alarm	Attributes	Applicable major release
Name: OESECSwitchOver (9042) Type: equipmentAlarm Package: equipment.OESECSwitchOver Raised on class: equipment.BaseCard	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ECEventSwitchover	Release: • N/A
Description: The alarm is raised when a OES EC Switch over happens.		
Remedial action: Informational - OES Equipment Controller Switch over		

Table 39-644 OesFan32HReqd

Alarm	Attributes	Applicable major release
Name: OesFan32HReqd (9044) Type: equipmentAlarm Package: equipment.OesFan32HReqd Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: oesFan32HReqd	Release: • N/A
Description: The alarm is raised when the OES chassis in a PSS32 shelf requires high speed fan (FAN32H), but the fan inserted is not the right type.		
Remedial action: Replace the OES fan unit with the correct one for 1830 PSS32 shelf.		

Table 39-645 OesFanFailure

Alarm	Attributes	Applicable major release
Name: OesFanFailure (9045) Type: equipmentAlarm Package: equipment.OesFanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • N/A
Description: The alarm is raised when the associated fan in the OES chassis is not operationally Up.		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 39-646 OesFanSpeedHigh

Alarm	Attributes	Applicable major release
Name: OesFanSpeedHigh (11106) Type: equipmentAlarm Package: equipment.OesFanSpeedHigh Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: oesFanSpeedHigh	Release: • N/A
Description: The alarm is raised when the fan speed of the OES chassis is too high.		
Remedial action: Remove and re-insert the fan tray into the chassis. If the alarm does not clear, replace the fan tray.		

Table 39-647 OesFanSpeedLow

Alarm	Attributes	Applicable major release
Name: OesFanSpeedLow (11107) Type: equipmentAlarm Package: equipment.OesFanSpeedLow Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: oesFanSpeedLow	Release: • N/A
Description: The alarm is raised when the fan speed of the OES chassis is too low.		
Remedial action: Check for airflow blockage or a dirty filter, and clear. If the alarm does not clear, replace the fan tray.		

Table 39-648 OesFirmwareCondition

Alarm	Attributes	Applicable major release
Name: OesFirmwareCondition (11108) Type: firmwareAlarm Package: equipment.OesFirmwareCondition Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FirmwareCondition	Release: • N/A
Description: The OesFirmwareCondition alarm is generated when the firmware on the card has a condition that needs to be notified.		
Remedial action: The OesFirmwareCondition alarm is generated when the firmware on the card has a condition that needs to be notified to network administrator.		

Table 39-649 OesNtpOutOfSync

Alarm	Attributes	Applicable major release
Name: OesNtpOutOfSync (11109) Type: equipmentAlarm Package: equipment.OesNtpOutOfSync Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesNtpOutOfSync	Release: • N/A
Description: This alarm is generated when NTP time on the OES is not synchronized to the host router.		
Remedial action: Ensure the host router has NTP configured and a reachable time source. Allow 40 minutes for the condition to clear.		

Table 39-650 OesPortError

Alarm	Attributes	Applicable major release
Name: OesPortError (9046) Type: equipmentAlarm Package: equipment.OesPortError Raised on class: equipment.PhysicalPort	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesPortDeviceorPortFailure-Detected	Release: • N/A
Description: This alarm is generated when there is a failure on the device or the transmission of the OES port.		
Remedial action: There is a device or transmission failure on the OES port, this could be service affecting. Please try taking the port out of service then bringing back in service, eg. shutdown/no shutdown , or try a soft reset, hard reset, then replacement of the card if the error condition persists.		

Table 39-651 OesPowerSupplyFailure

Alarm	Attributes	Applicable major release
Name: OesPowerSupplyFailure (9047) Type: equipmentAlarm Package: equipment.OesPowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • N/A
Description: The alarm is raised when a power filter card reports a failure.		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-652 oesSwBelowMinRev

Alarm	Attributes	Applicable major release
Name: oesSwBelowMinRev (11182) Type: equipmentAlarm Package: netw.oesSwBelowMinRev Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OesSwBelowMinRev	Release: • N/A

Table 39-652 oesSwBelowMinRev (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is generated when the version of the running OES software image is below the minimum expected version.		
Remedial action: Upgrade the OES to a software image that is equal to or greater than the minimum expected version.		

Table 39-653 oesSwUpgdCleanupFailed

Alarm	Attributes	Applicable major release
Name: oesSwUpgdCleanupFailed (11183) Type: equipmentAlarm Package: netw.oesSwUpgdCleanupFailed Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OesSwUpgdCleanupFailed	Release: • N/A
Description: This alarm is generated when the operation to clean-up a failed software upgrade fails.		
Remedial action: 1. Determine the reason for the upgrade failure from tmnxOesEventReason in the notification. First clear the condition indicated by the reason. 2. Re-try the upgrade procedure. 3. Contact the Nokia technical support team if the re-try does not fix the problem.		

Table 39-654 oesSwUpgdFailed

Alarm	Attributes	Applicable major release
Name: oesSwUpgdFailed (11184) Type: equipmentAlarm Package: netw.oesSwUpgdFailed Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OesSwUpgdFailed	Release: • N/A
Description: This alarm is generated when a failure occurs in upgrading a component in the OES.		
Remedial action: 1.Determine the reason the upgrade failed by checking the tmnxOesEventReason. First clear the condition indicated by the reason in the object tmnxOesEventReason. 2. Perform a soft reset on the card that failed to upgrade and try the upgrade procedure again. 3. Perform a hard reset on the card that failed to upgrade and try the upgrade procedure again. 4. Remove and re-insert the card that failed to upgrade and try the upgrade procedure again. 5. Replace the card that failed to upgrade and try the upgrade procedure again. 6. Inform the Nokia technical support team.		

Table 39-655 OesUsrpnlPortDown

Alarm	Attributes	Applicable major release
Name: OesUsrpnlPortDown (9048) Type: equipmentAlarm Package: equipment.OesUsrpnlPortDown Raised on class: equipment.PhysicalPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OesUsrpnlPortDown	Release: • N/A
Description: This alarm is generated when a port (E1 or E2) on an OES USRPNL card is not operational.		

Table 39-655 OesUsrpnlPortDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The port on OES User panel may be misconnected, disconnected, faulty or having faulty cable faulty User Panel card. Check that the cable is correctly connected and test the cable.		

Table 39-656 OlcStateChangeAlarm

Alarm	Attributes	Applicable major release
Name: OlcStateChangeAlarm (3740) Type: communicationsAlarm Package: generic.OlcStateChangeAlarm Raised on class: generic.GenericObject	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unknown	Release: • N/A
Description: The alarm is raised to notify the user, when an OLC State change takes place at the specified revert time.		
Remedial action: Informational - This is a notification alarm to indicate that the object will revert it's OLC state.		

Table 39-657 OldArchiveLogsDeleted

Alarm	Attributes	Applicable major release
Name: OldArchiveLogsDeleted (198) Type: databaseAlarm Package: db.OldArchiveLogsDeleted Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: archivedLogsIssue	Release: • N/A
Description: The alarm is raised when the 5620 SAM deletes the applied archive logs because database disk space is low. In a standalone deployment, the 5620 SAM deletes all archive logs. In a redundant deployment, the 5620 SAM deletes the applied archive logs, and can raise the alarm against the primary or standby database.		
Remedial action: Informational - verify there is adequate disk space for the archive log files on the database servers. If the alarm persists then the frequency of database backups should be increased.		

Table 39-658 OMSTrailDown

Alarm	Attributes	Applicable major release
Name: OMSTrailDown (8082) Type: communicationsAlarm Package: optical.OMSTrailDown Raised on class: optical.OMSTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when termination point(s) of the OMS trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-659 OneWayCommunication

Alarm	Attributes	Applicable major release
Name: OneWayCommunication (733) Type: communicationsAlarm Package: server.OneWayCommunication Raised on class: server.AuxiliaryServer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routingConfiguration	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server, but the auxiliary server can communicate with the main server.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 39-660 OperDownInvalidMac

Alarm	Attributes	Applicable major release
Name: OperDownInvalidMac (8144) Type: configurationAlarm Package: srrp.OperDownInvalidMac Raised on class: srrp.Instance	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidMacAddress	Release: • N/A
Description: This Alarm is generated when the operational virtual MAC of an SRRP instance conflicts with the MAC of the parent interface.		
Remedial action: The alarm is generated when the operational virtual MAC of an SRRP instance conflicts with the MAC of the parent interface. The SRRP virtual router instance is not allowed to become operationally 'up'.		

Table 39-661 OperDownInvalidMacClear

Alarm	Attributes	Applicable major release
Name: OperDownInvalidMacClear (8145) Type: configurationAlarm Package: srrp.OperDownInvalidMacClear Raised on class: srrp.Instance	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidMacAddressCleared	Release: • N/A
Description: The Alarm is generated when a previously occurring OperDownInvalidMac notification has been cleared. Operational virtual MAC of an IPv4 SRRP instance does not have any conflict with the MAC of the parent interface.		
Remedial action: The alarm is generated when a previously occurring OperDownInvalidMac notification has been cleared. Operational virtual MAC of an IPv4 SRRP instance does not have any conflict with the MAC of the parent interface.		

Table 39-662 OpticalAmplifierLossOfInputOpticalPower

Alarm	Attributes	Applicable major release
Name: OpticalAmplifierLossOfInputOpticalPower (1185) Type: communicationsAlarm Package: ethernetequipment. OpticalAmplifierLossOfInputOpticalPower Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierLossOfInputOpticalPower	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Loss of input optical power on an optical amplifier interface.		
Remedial action: Ensure that the input optical power at the face plate is greater than the minimum required		

Table 39-663 OpticalAmplifierLossOfOutputPower

Alarm	Attributes	Applicable major release
Name: OpticalAmplifierLossOfOutputPower (1186) Type: communicationsAlarm Package: ethernetequipment. OpticalAmplifierLossOfOutputPower Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierLossOfOutputPower	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Loss of output power on an optical amplifier interface.		
Remedial action: If the alarm is persistent: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-664 OPticalAmplifierModuleCaseTemperatureHigh

Alarm	Attributes	Applicable major release
Name: OPticalAmplifierModuleCaseTemperatureHigh (1180) Type: communicationsAlarm Package: ethernetequipment. OPticalAmplifierModuleCaseTemperatureHigh Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierModuleCaseTemperatureHigh	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Module Case Temperature High on an optical amplifier interface.		
Remedial action: Decrease the ambient temperature		

Table 39-665 OPticalAmplifierModuleCaseTemperatureLow

Alarm	Attributes	Applicable major release
Name: OPticalAmplifierModuleCaseTemperatureLow (1181) Type: communicationsAlarm Package: ethernetequipment. OPticalAmplifierModuleCaseTemperatureLow Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierModuleCaseTemperatureLow	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Module Case Temperature Low on an optical amplifier interface.		
Remedial action: Increase the ambient temperature		

Table 39-666 OpticalAmplifierModuleCommunicationFailure

Alarm	Attributes	Applicable major release
Name: OpticalAmplifierModuleCommunicationFailure (1187) Type: communicationsAlarm Package: ethernetequipment. OpticalAmplifierModuleCommunicationFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierModuleCommunicationFailure	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Module Communication Failure on a tunable dispersion compensation module's interface.		
Remedial action: If the alarm is persistent: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-667 OpticalAmplifierPumpCurrent

Alarm	Attributes	Applicable major release
Name: OpticalAmplifierPumpCurrent (1188) Type: communicationsAlarm Package: ethernetequipment. OpticalAmplifierPumpCurrent Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierPumpcurrent	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Pump over current on an optical amplifier interface.		
Remedial action: If the alarm is persistent: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-668 OPticalAmplifierPumpTemperature

Alarm	Attributes	Applicable major release
Name: OPticalAmplifierPumpTemperature (1182) Type: communicationsAlarm Package: ethernetequipment. OPticalAmplifierPumpTemperature Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AmplifierPumpTemperature	Release: • N/A
Description: The alarm is raised when a device reports an Amplifier Pump Temperature on an optical amplifier interface.		
Remedial action: Decrease the ambient temperature		

Table 39-669 OpticalTdcmEEPROMinvalid

Alarm	Attributes	Applicable major release
Name: OpticalTdcmEEPROMinvalid (1189) Type: communicationsAlarm Package: ethernetequipment. OpticalTdcmEEPROMinvalid Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmEEPROMinvalid	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm EEPROM invalid on a tunable dispersion compensation module's interface.		
Remedial action: Replace the card		

Table 39-670 OpticalTdcmModuleCommunicationFailure

Alarm	Attributes	Applicable major release
Name: OpticalTdcmModuleCommunicationFailure (1190) Type: communicationsAlarm Package: ethernetequipment. OpticalTdcmModuleCommunicationFailure Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmModuleCommunication-Failure	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Module Communication Failure on a tunable dispersion compensation module's interface.		
Remedial action: If the alarm is persistent: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-671 OPticalTdcmModuleTemperatureHigh

Alarm	Attributes	Applicable major release
Name: OPticalTdcmModuleTemperatureHigh (1183) Type: communicationsAlarm Package: ethernetequipment.OPticalTdcmModuleTemperatureHigh Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmModuleTemperatureHigh	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Module Temperature High on a tunable dispersion compensation module's interface.		
Remedial action: Decrease the ambient temperature		

Table 39-672 OPticalTdcmModuleTemperatureLow

Alarm	Attributes	Applicable major release
Name: OPticalTdcmModuleTemperatureLow (1184) Type: communicationsAlarm Package: ethernetequipment.OPticalTdcmModuleTemperatureLow Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmModuleTemperatureLow	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Module Temperature Low on a tunable dispersion compensation module's interface.		
Remedial action: Increase the ambient temperature		

Table 39-673 OpticalTdcmNotReady

Alarm	Attributes	Applicable major release
Name: OpticalTdcmNotReady (1191) Type: communicationsAlarm Package: ethernetequipment.OpticalTdcmNotReady Raised on class: ethernetequipment.WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmNotReady	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Not Ready on a tunable dispersion compensation module's interface.		
Remedial action: This is a transient condition that should clear under normal operation but if it causes the link to fail and persists: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-674 OpticalTdcmThermalControlTemperatureLimit

Alarm	Attributes	Applicable major release
Name: OpticalTdcmThermalControlTemperatureLimit (1192) Type: communicationsAlarm Package: ethernetequipment. OpticalTdcmThermalControlTemperatureLimit Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmThermalControlTemperatureLimit	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Thermal Control Temperature Limit on a tunable dispersion compensation module's interface.		
Remedial action: If this alarm persists: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-675 OpticalTdcmThermalControlUnlocked

Alarm	Attributes	Applicable major release
Name: OpticalTdcmThermalControlUnlocked (1193) Type: communicationsAlarm Package: ethernetequipment. OpticalTdcmThermalControlUnlocked Raised on class: ethernetequipment. WaveLengthTracker	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TdcmThermalControlUnlocked	Release: • N/A
Description: The alarm is raised when a device reports a Tdcm Thermal Control Unlocked on a tunable dispersion compensation module's interface.		
Remedial action: This is a transient condition that should clear under normal operation but if it causes the link to fail and persists: 1. clear the mda, 2. clear card 3. replace the card		

Table 39-676 OracleHomeDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: OracleHomeDiskSpaceBelowThreshold (399) Type: databaseAlarm Package: db.OracleHomeDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the primary or standalone database Oracle disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The Oracle Proxy purges the log based on database file policy configuration. Reducing the number of archives to keep and/or size of the log files or increasing the available disk space will resolve the problem. If alarm persists please contact your Nokia support representative for assistance.		

Table 39-677 OspfAdvRtrLsaLimitWarning

Alarm	Attributes	Applicable major release
Name: OspfAdvRtrLsaLimitWarning (9585) Type: configurationAlarm Package: ospf.OspfAdvRtrLsaLimitWarning Raised on class: ospf.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: AdvRtrLsaLimitWarning	Release: • N/A
Description: The alarm is raised when when OSPF reaches Advertise Router LSA limit value or warning limit.		
Remedial action: Increase the LSA Limit or LSA Threshold for this OSPF instance.		

Table 39-678 OspfExportLimitDropped

Alarm	Attributes	Applicable major release
Name: OspfExportLimitDropped (1924) Type: configurationAlarm Package: ospf.OspfExportLimitDropped Raised on class: ospf.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitDropped	Release: • N/A
Description: The alarm is raised when the total number of exported routes to the OSPF level, drops below the configured limit.		
Remedial action: Informational - the total number of exported routes from the route table to this OSPF level drops below the configured export limit.		

Table 39-679 OspfExportLimitReached

Alarm	Attributes	Applicable major release
Name: OspfExportLimitReached (1925) Type: configurationAlarm Package: ospf.OspfExportLimitReached Raised on class: ospf.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitReached	Release: • N/A
Description: The alarm is raised when the total number of routes to the OSPF level is equal to the configured limit for exported routes.		
Remedial action: Informational - the total number of routes for the level is equal to the configured limit for exported routes		

Table 39-680 OspfExportLimitWarning

Alarm	Attributes	Applicable major release
Name: OspfExportLimitWarning (1926) Type: configurationAlarm Package: ospf.OspfExportLimitWarning Raised on class: ospf.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitWarning	Release: • N/A
Description: The alarm is raised when the total number of exported routes to the OSPF level is equal to the configured percentage, vRtrIsisExportLimitLogPercent of the export limit.		

Table 39-680 OspfExportLimitWarning (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - the total number of exported routes or the level is equal to the configured Export Limit Log Percent		

Table 39-681 OspfExternalLsaThresholdExceeded

Alarm	Attributes	Applicable major release
Name: OspfExternalLsaThresholdExceeded (372) Type: topologyAlarm Package: topology. OspfExternalLsaThresholdExceeded Raised on class: topology.Cpaa	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: manyExternalLSAsFloodingIn-toIGP	Release: • N/A
Description: The alarm is raised when the number of OSPF external LSAs exceeds the maximum threshold because a large number of external LSAs flooding into the IGP.		
Remedial action: User configured alarm for monitoring purpose. The advertised external routes can be viewed using CPAM IGP prefix list.		

Table 39-682 OspfIfTxRetransmit

Alarm	Attributes	Applicable major release
Name: OspfIfTxRetransmit (662) Type: communicationsAlarm Package: ospf.OspfIfTxRetransmit Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hello Applicable probable causes: • hello • dbDescript • lsReq • lsUpdate • lsAck • nullPacket	Release: • N/A
Description: The alarm is raised when an NE retransmits an OSPF packet. The alarm information includes the NE ID of the OSPF neighbor. The alarm is not raised against a Release 4.0 or later NE.		
Remedial action: Informational - an NE retransmits an OSPF packet. The alarm information includes the NE ID of the OSPF neighbor. The alarm is not raised against a Release 4.0 or later NE.		

Table 39-683 OspfInternalLsaRateThresholdExceededPerArea

Alarm	Attributes	Applicable major release
Name: OspfInternalLsaRateThreshold-ExceededPerArea (310) Type: topologyAlarm Package: topology.OspfInternalLsaRateThresholdExceededPerArea Raised on class: topology.Area	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableIGPNetwork	Release: • N/A
Description: The alarm is raised when the OSPF internal LSA rate for an area exceeds the maximum allowed value because of an unstable IGP network.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-684 OspfInternalLsaThresholdExceededPerArea

Alarm	Attributes	Applicable major release
Name: OspfInternalLsaThresholdExceededPerArea (309) Type: topologyAlarm Package: topology.OspfInternalLsaThresholdExceededPerArea Raised on class: topology.Area	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: largeIgpNetwork	Release: • N/A
Description: The alarm is raised when the number of OSPF internal LSAs for an area exceeds the maximum allowed value because of a large IGP network.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-685 OspfLsaRateThresholdExceededPerRouter

Alarm	Attributes	Applicable major release
Name: OspfLsaRateThresholdExceededPerRouter (308) Type: topologyAlarm Package: topology.OspfLsaRateThresholdExceededPerRouter Raised on class: topology.Router	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unstableLinksOnRouter	Release: • N/A
Description: The alarm is raised when the OSPF LSA rate for an NE exceeds the maximum allowed value because of an unstable NE link.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-686 OspfLsaThresholdExceededPerRouter

Alarm	Attributes	Applicable major release
Name: OspfLsaThresholdExceededPerRouter (374) Type: topologyAlarm Package: topology. OspfLsaThresholdExceededPerRouter Raised on class: topology.Router	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routerAdvertisingManyLSAs	Release: • N/A
Description: The alarm is raised when the number of OSPF LSAs for an NE exceeds the maximum allowed value because the NE advertises too many LSAs.		
Remedial action: User configured alarm for monitoring purpose. IGP historical map can be used for debugging purpose.		

Table 39-687 OspfSIDError

Alarm	Attributes	Applicable major release
Name: OspfSIDError (9586) Type: configurationAlarm Package: ospf.OspfSIDError Raised on class: ospf.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ospfSIDError	Release: • N/A
Description: This notification is generated when OSPF receives a SID label which is already in use for another prefix.		
Remedial action: In case of system exhaustion, the IGP instance goes into overload. The operator must manually clear the IGP overload condition after freeing resources. IGP will attempt to program at the next SPF all tunnels which previously failed the programming operation		

Table 39-688 OspfSIDNotInLabelRange

Alarm	Attributes	Applicable major release
Name: OspfSIDNotInLabelRange (9587) Type: configurationAlarm Package: ospf.OspfSIDNotInLabelRange Raised on class: ospf.Site	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ospfSIDNotInLabelRange	Release: • N/A
Description: This notification is generated when OSPF receives a SID which is not within the label range of the next hop router.		
Remedial action: The SID range needs to be change to include remote SID received.		

Table 39-689 OTSTrailDown

Alarm	Attributes	Applicable major release
Name: OTSTrailDown (8084) Type: communicationsAlarm Package: optical.OTSTrailDown Raised on class: optical.OTSTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A

Table 39-689 OTSTrailDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the termination point(s) of the OTS trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-690 OTUAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: OTUAlarmIndicationSignal (755) Type: communicationsAlarm Package: ethernetequipment. OTUAlarmIndicationSignal Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: AlarmIndicationSignal	Release: • N/A
Description: The alarm is raised when a device reports an AIS on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-691 OTUBackwardDefectIndication

Alarm	Attributes	Applicable major release
Name: OTUBackwardDefectIndication (756) Type: communicationsAlarm Package: ethernetequipment. OTUBackwardDefectIndication Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackwardDefectIndication	Release: • N/A
Description: The alarm is raised when a device reports a BDI on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-692 OTUBackwardIncomingAlignmentError

Alarm	Attributes	Applicable major release
Name: OTUBackwardIncomingAlignmentError (815) Type: communicationsAlarm Package: ethernetequipment. OTUBackwardIncomingAlignmentError Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BackwardIncomingAlignment-Error	Release: • N/A
Description: The alarm is raised when a device reports an ODU alarm indication signal on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-693 OTUBitErrorRateSignalDegradation

Alarm	Attributes	Applicable major release
Name: OTUBitErrorRateSignalDegradation (757) Type: communicationsAlarm Package: ethernetequipment. OTUBitErrorRateSignalDegradation Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BitErrorRateSignalDegrada-tion	Release: • N/A
Description: The alarm is raised when a device reports a BER-SD on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-694 OTUBitErrorRateSignalFail

Alarm	Attributes	Applicable major release
Name: OTUBitErrorRateSignalFail (758) Type: communicationsAlarm Package: ethernetequipment. OTUBitErrorRateSignalFail Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BitErrorRateSignalFail	Release: • N/A
Description: The alarm is raised when a device reports a BER-SF on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-695 OTUFECRxTxModeMismatch

Alarm	Attributes	Applicable major release
Name: OTUFECRxTxModeMismatch (759) Type: communicationsAlarm Package: ethernetequipment. OTUFECRxTxModeMismatch Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FECRxTxModeMismatch	Release: • N/A
Description: The alarm is raised when a device reports a FEC Rx/Tx mode mismatch on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-696 OTUFECSignalDegradation

Alarm	Attributes	Applicable major release
Name: OTUFECSignalDegradation (760) Type: communicationsAlarm Package: ethernetequipment. OTUFECSignalDegradation Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FECSignalDegradation	Release: • N/A
Description: The alarm is raised when a device reports a FEC-SD on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-697 OTUFECSignalFailure

Alarm	Attributes	Applicable major release
Name: OTUFECSignalFailure (761) Type: communicationsAlarm Package: ethernetequipment.OTUFECSignalFailure Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FECSignalFailure	Release: • N/A
Description: The alarm is raised when a device reports a FEC-SF on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-698 OTUIncomingAlignmentError

Alarm	Attributes	Applicable major release
Name: OTUIncomingAlignmentError (816) Type: communicationsAlarm Package: ethernetequipment. OTUIncomingAlignmentError Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: IncomingAlignmentError	Release: • N/A
Description: The alarm is raised when a device reports an ODU open connection indication on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-699 OTULossOfClock

Alarm	Attributes	Applicable major release
Name: OTULossOfClock (762) Type: communicationsAlarm Package: ethernetequipment.OTULossOfClock Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfClock	Release: • N/A
Description: The alarm is raised when a device reports an LOC on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-700 OTULossOfFraming

Alarm	Attributes	Applicable major release
Name: OTULossOfFraming (763) Type: communicationsAlarm Package: ethernetequipment.OTULossOfFraming Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfFraming	Release: • N/A
Description: The alarm is raised when a device reports an LOF on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-701 OTULossOfMultiFrame

Alarm	Attributes	Applicable major release
Name: OTULossOfMultiFrame (764) Type: communicationsAlarm Package: ethernetequipment.OTULossOfMultiFrame Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfMultiFrame	Release: • N/A
Description: The alarm is raised when a device reports an LOM on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-702 OTULossOfSignal

Alarm	Attributes	Applicable major release
Name: OTULossOfSignal (765) Type: communicationsAlarm Package: ethernetequipment.OTULossOfSignal Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LossOfSignal	Release: • N/A
Description: The alarm is raised when a device reports an LOS on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-703 OTUODUAlarmIndicationSignal

Alarm	Attributes	Applicable major release
Name: OTUODUAlarmIndicationSignal (766) Type: communicationsAlarm Package: ethernetequipment. OTUODUAlarmIndicationSignal Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ODUAlarmIndicationSignal	Release: • N/A
Description: The alarm is raised when a device reports an ODU AIS on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-704 OTUODULocked

Alarm	Attributes	Applicable major release
Name: OTUODULocked (767) Type: communicationsAlarm Package: ethernetequipment.OTUODULocked Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ODULocked	Release: • N/A
Description: The alarm is raised when a device reports an ODU locked on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-705 OTUODUOpenConnectionIndication

Alarm	Attributes	Applicable major release
Name: OTUODUOpenConnectionIndication (768) Type: communicationsAlarm Package: ethernetequipment. OTUODUOpenConnectionIndication Raised on class: ethernetequipment.OtuInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ODUOpenConnectionIndication	Release: • N/A
Description: The alarm is raised when a device reports an ODU-OCI on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-706 OTUOPUPSIPayloadTypeMismatch

Alarm	Attributes	Applicable major release
Name: OTUOPUPSIPayloadTypeMismatch (817) Type: communicationsAlarm Package: ethernetequipment. OTUOPUPSIPayloadTypeMismatch Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OPUPSIPayloadTypeMismatch	Release: • N/A
Description: The alarm is raised when a device reports a PM backward defect indication on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-707 OTUOPUPSITraceMismatch

Alarm	Attributes	Applicable major release
Name: OTUOPUPSITraceMismatch (818) Type: communicationsAlarm Package: ethernetequipment. OTUOPUPSITraceMismatch Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OPUPSITraceMismatch	Release: • N/A
Description: The alarm is raised when a device reports an ODU locked indication on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-708 OTUPMBackwardDefectIndication

Alarm	Attributes	Applicable major release
Name: OTUPMBackwardDefectIndication (769) Type: communicationsAlarm Package: ethernetequipment. OTUPMBackwardDefectIndication Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PMBackwardDefectIndication	Release: • N/A
Description: The alarm is raised when a device reports a PM BDI on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-709 OTUPMTraceIDMismatch

Alarm	Attributes	Applicable major release
Name: OTUPMTraceIDMismatch (819) Type: communicationsAlarm Package: ethernetequipment. OTUPMTraceIDMismatch Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PMTraceIDMismatch	Release: • N/A
Description: The alarm is raised when a device reports an ODU open connection indication on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-710 OTUTraceIdMismatch

Alarm	Attributes	Applicable major release
Name: OTUTraceIdMismatch (820) Type: communicationsAlarm Package: ethernetequipment.OTUTraceIdMismatch Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TraceIdMismatch	Release: • N/A
Description: The alarm is raised when a device reports a trace ID mismatch on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-711 OTUTrailDown

Alarm	Attributes	Applicable major release
Name: OTUTrailDown (5126) Type: communicationsAlarm Package: optical.OTUTrailDown Raised on class: optical.OTUTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the OTU trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-712 OTUTrailMisConfigured

Alarm	Attributes	Applicable major release
Name: OTUTrailMisConfigured (5127) Type: communicationsAlarm Package: optical.OTUTrailMisConfigured Raised on class: optical.OTUTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: OchCrossConnectionTrail-NameMisMatch	Release: • N/A
Description: The alarm is raised when all the OCh cross connections (XCs) of an OTU trail do not have the same trail name. In order for the auto wavekey processing to work properly, the XC name should be the same on all NEs of the OTU trail.		
Remedial action: Recreate the OCH Cross Connects with same Trail name else Wave Tracker does not work properly.		

Table 39-713 OTUUncorrectableFECErrors

Alarm	Attributes	Applicable major release
Name: OTUUncorrectableFECErrors (770) Type: communicationsAlarm Package: ethernetequipment. OTUUncorrectableFECErrors Raised on class: ethernetequipment.OtuInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UncorrectableFECErrors	Release: • N/A
Description: The alarm is raised when a device reports one or more uncorrectable FEC errors on an OTU-enabled interface.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-714 OutOfBandManagementConnectionDown

Alarm	Attributes	Applicable major release
Name: OutOfBandManagementConnectionDown (138) Type: communicationsAlarm Package: netw. OutOfBandManagementConnectionDown Raised on class: netw.NodeDiscoveryControl	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: managementConnectionDown	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function over an out-of-band connection.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM.		

Table 39-715 OutOfSlots

Alarm	Attributes	Applicable major release
Name: OutOfSlots (462) Type: configurationAlarm Package: equipment.OutOfSlots Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: noAvailableSlotNumbers	Release: • N/A
Description: The alarm is raised when a stack element enters pass-through mode because there is no slot number for the element.		
Remedial action: Login to switch console, correct the slot number and reload stack.		

Table 39-716 PacingInProgressWarning

Alarm	Attributes	Applicable major release
Name: PacingInProgressWarning (737) Type: configurationAlarm Package: tunnelmgmt.PacingInProgressWarning Raised on class: tunnelmgmt.TopologyRule	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: noUpdatesDueToPacingIn-Progress	Release: • N/A
Description: The alarm is raised when tunnel creation or deletion is not performed after a member is added or removed from a rule group because topology rule pacing is in progress. When this occurs, the Reapply and Delete Unused operations must be performed manually when the pacing is complete. The alarm clears after a Reapply operation is performed.		
Remedial action: When this occurs, the Reapply and Delete Unused operations must be performed manually when the pacing is complete. The alarm clears after a Reapply operation is performed.		

Table 39-717 PacketDropped

Alarm	Attributes	Applicable major release
Name: PacketDropped (11070) Type: configurationAlarm Package: dhcp.PacketDropped Raised on class: dhcp.AbstractDhcpServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: DhcpsPacketDropped	Release: • N/A
Description: The alarm is generated when a DHCP or DHCPv6 server instance dropped a DHCP packet it received.		
Remedial action: The recovery action, if any, will depend on the reason.		

Table 39-718 ParentTemplateInvalid

Alarm	Attributes	Applicable major release
Name: ParentTemplateInvalid (194) Type: configurationAlarm Package: template.ParentTemplateInvalid Raised on class: template.TemplateBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: referencedObjectInvalid	Release: • N/A
Description: The alarm is raised when a parent template in a template binding is invalid. The alarm is deprecated in the 5620 SAM, Release 6.0 and later.		
Raising condition: ('parentTemplateInvalidReference' EQUAL 'true')		
Clearing condition: ('parentTemplateInvalidReference' EQUAL 'false')		
Remedial action: Informational - deprecated 6.0		

Table 39-719 PatchLevelMismatch

Alarm	Attributes	Applicable major release
Name: PatchLevelMismatch (659) Type: softwareAlarm Package: netw.PatchLevelMismatch Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: patchLevelMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM primary main server software patch level does not match the standby main server software patch level.		
Remedial action: Informational - it is advisable to have both active and standby servers at the same patch level. During a maintenance window apply the appropriate patch to the standby server to bring it inline with the main server.		

Table 39-720 PathReoptimized

Alarm	Attributes	Applicable major release
Name: PathReoptimized (28) Type: pathAlarm Package: mpls.PathReoptimized Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: pathReoptimized	Release: • N/A
Description: The alarm is raised when an MPLS path generates an mplsTunnelReoptimized trap.		
Remedial action: Informational only.		

Table 39-721 PathRerouted

Alarm	Attributes	Applicable major release
Name: PathRerouted (29) Type: pathAlarm Package: mpls.PathRerouted Raised on class: mpls.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: pathRerouted	Release: • N/A
Description: The alarm is raised when an MPLS path generates an mplsTunnelRerouted trap.		
Remedial action: Informational only.		

Table 39-722 PbbSiteMisconfiguration

Alarm	Attributes	Applicable major release
Name: PbbSiteMisconfiguration (571) Type: configurationAlarm Package: vpls.PbbSiteMisconfiguration Raised on class: vpls.AbstractVpls	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: includeBothBAndISite	Release: • N/A
Description: The alarm is raised when a VPLS contains a B-Site and an I-Site.		

Table 39-722 PbbSiteMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Include B-Site(s)' EQUAL 'true') AND ('Include I-Site(s)' EQUAL 'true'))		
Clearing condition: (('Include B-Site(s)' NOT EQUAL 'true') OR ('Include I-Site(s)' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which needs to be corrected. The service can have only an I-site or a B-site but not both.		

Table 39-723 PChipCAMEvent

Alarm	Attributes	Applicable major release
Name: PChipCAMEvent (814) Type: hardwareAnomaly Package: equipment.PChipCAMEvent Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: camError	Release: • N/A
Description: The alarm is raised when an IOM or CPM experiences a P-chip CAM error.		
Remedial action: Informational - if the condition persists then the card indicated in the alarm should be replaced.		

Table 39-724 PChipError

Alarm	Attributes	Applicable major release
Name: PChipError (593) Type: hardwareAnomaly Package: equipment.PChipError Raised on class: equipment.BaseCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pChipError	Release: • N/A
Description: The alarm is raised when persistent FCS errors are detected on the specified complex in the specified direction.		
Remedial action: A fault has been detected in the hardware. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-725 PChipMemoryEvent

Alarm	Attributes	Applicable major release
Name: PChipMemoryEvent (608) Type: hardwareAnomaly Package: equipment.PChipMemoryEvent Raised on class: equipment.BaseCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: memoryParityError	Release: • N/A
Description: The alarm is raised when a P chip detects a memory parity error. The alarm is raised against a 7450 ESS, 7710 SR, or 7750 SR. The alarm is raised against a Release 6.0 NE at R10 or later and a Release 6.1 NE at R5 or later.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-726 PeerGroupDynamicPeerLimitReached

Alarm	Attributes	Applicable major release
Name: PeerGroupDynamicPeerLimitReached (9031) Type: ProtocolAlarm Package: bgp.PeerGroupDynamicPeerLimitReached Raised on class: bgp.PeerGroup	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: peerGroupDynamicPeerLimitReached	Release: • N/A
Description: The alarm is raised when the dynamic peer limit for this BGP Group is reached.		
Remedial action: Increase the dynamic peer limit for this BGP group.		

Table 39-727 peerSetConfigurationIssue

Alarm	Attributes	Applicable major release
Name: peerSetConfigurationIssue (267) Type: configurationAlarm Package: pim.peerSetConfigurationIssue Raised on class: pim.VirtualAnyCastRP	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mismatchPeerSets	Release: • N/A
Description: The alarm is raised when a peer set is misconfigured.		
Remedial action: A configuration error has occurred that must be corrected. Please check the global Virtual Anycast RP configuration and its operational status flag so that the Inconsistent Peer Sets and Only one peer bits are reset.		

Table 39-728 PeerToAuxAddressMismatch

Alarm	Attributes	Applicable major release
Name: PeerToAuxAddressMismatch (8408) Type: configurationAlarm Package: server.PeerToAuxAddressMismatch Raised on class: server.SamServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: peerToAuxAddressMismatch	Release: • N/A
Description: The alarm is raised when standbyAddress in cluster in a 5620 SAM main server configuration does not match the same property on standby configuration.		
Remedial action: A configuration error has been made which must be corrected. The standbyAddress in cluster on primary server does not match the standby address accessible to Auxiliary servers, and must be corrected.		

Table 39-729 PersistenceRestoreProblem

Alarm	Attributes	Applicable major release
Name: PersistenceRestoreProblem (5141) Type: processingErrorAlarm Package: sw.PersistenceRestoreProblem Raised on class: sw.NodePersistence	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: persistenceRestoreProblem	Release: • N/A

Table 39-729 PersistenceRestoreProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an error is detected while processing a persistence record.		
Remedial action: Check the node persistence configuration.		

Table 39-730 PersistencyFileSysThresRaised

Alarm	Attributes	Applicable major release
Name: PersistencyFileSysThresRaised (5142) Type: equipmentAlarm Package: sw.PersistencyFileSysThresRaised Raised on class: sw.NodePersistence	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistencyFileSysThres-Raised	Release: • N/A
Description: The alarm is raised when the filesystem reaches 90 percent usage.		
Remedial action: Delete unnecessary files on the compact flash disk. This operation must be executed using CLI interface on the NE.		

Table 39-731 PkiCertVerificationFailed

Alarm	Attributes	Applicable major release
Name: PkiCertVerificationFailed (3743) Type: configurationAlarm Package: ipsec.PkiCertVerificationFailed Raised on class: ipsec.IPSecBaseEntity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pkiCertInvalid	Release: • N/A
Description: The alarm is raised when an attempt to verify the certificate fails.		
Remedial action: An attempt to verify the certificate fails. Please make sure the certificate specified exists under the node cf3:system-pki and is a valid certificate		

Table 39-732 PkiFileReadFailed (sitesec)

Alarm	Attributes	Applicable major release
Name: PkiFileReadFailed (3744) Type: configurationAlarm Package: sitesec.PkiFileReadFailed Raised on class: sitesec.CertificateAuthProfile	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pkiFileReadCorrupted	Release: • N/A
Description: The alarm is raised when an attempt to read the file fails.		
Remedial action: An attempt to read the PKI file fails. Please make sure the path specified is correct and the file exists under the node cf3:system-pki		

Table 39-733 PkiFileReadFailed (ipsec)

Alarm	Attributes	Applicable major release
Name: PkiFileReadFailed (3744) Type: configurationAlarm Package: ipsec.PkiFileReadFailed Raised on class: ipsec.IPSecBaseEntity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: pkiFileReadCorrupted	Release: • N/A
Description: The alarm is raised when an attempt to read the file fails.		
Remedial action: An attempt to read the PKI file fails. Please make sure the path specified is correct and the file exists under the node cf3:system-pki		

Table 39-734 PlcyAcctStatsEventOvrflw

Alarm	Attributes	Applicable major release
Name: PlcyAcctStatsEventOvrflw (5640) Type: equipmentAlarm Package: equipment.PlcyAcctStatsEventOvrflw Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PlcyAcctStatsPoolInUseExcAndLow	Release: • N/A
Description: The alarm is raised because of resource usage fluctuation that happens when the number of in-use stats resource usage exceeds 95 percent and deprecates below 85 percent of the specified stats pool limit more than 200 times.		
Remedial action: Notifications will resume once the resource usage fluctuation is in control i.e when the occurrence of tmnxPlcyAcctStatsPoolExcResource and tmnxPlcyAcctStatsPoolLowResource is less than 200.		

Table 39-735 PMFileRecovery

Alarm	Attributes	Applicable major release
Name: PMFileRecovery (4867) Type: communicationsAlarm Package: netw.PMFileRecovery Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: netconfDown	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server loses connectivity to an NE and as a result retrieves PM files that were not previously collected.		
Remedial action: Informational		

Table 39-736 PollDeadlineMissed

Alarm	Attributes	Applicable major release
Name: PollDeadlineMissed (240) Type: configurationAlarm Package: netw.PollDeadlineMissed Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyItemsToPoll	Release: • N/A
Description: The alarm is raised when a 5620 SAM server cannot finish browsing a statistics MIB before a polling interval expires.		
Remedial action: The rate at which performance statistics are being collected must be reduced or an AUX sever may be added to the 5620 SAM platform complex if the polling frequency cannot be reduced.		

Table 39-737 PoolManagerAddNewPoolFailed

Alarm	Attributes	Applicable major release
Name: PoolManagerAddNewPoolFailed (9593) Type: processingErrorAlarm Package: service.PoolManagerAddNewPoolFailed Raised on class: service.SubscriberInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerAddNewPool-Failed	Release: • N/A
Description: This notification is sent when adding a new pool, given by the DHCPv6 server, is failing. (Examples : conflict with existing pool, subnet too small, maximum number of pools reached, out of memory, etc.) [CAUSE] Failed to add a new pool given by the server. [EFFECT] The ISA-BB may run out of free DHCPv6 addresses or SLAAC prefixes. [RECOVERY] No recovery is needed. Retry periodically.		
Remedial action: No recovery is needed. Retry periodically.		

Table 39-738 PoolManagerCreateInternalObjectFailed

Alarm	Attributes	Applicable major release
Name: PoolManagerCreateInternalObjectFailed (9036) Type: processingErrorAlarm Package: dhcp. PoolManagerCreateInternalObjectFailed Raised on class: dhcp.Address6Pool	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerCreateInter-nalObjectFailed	Release: • N/A
Description: This notification is sent when the creation of an internal node object for a pool is failing. [CAUSE] Failed to create an internal object for a pool. [EFFECT] Forwarding will not work for UEs having an address/prefix from this pool. [RECOVERY] No recovery is needed. Retry periodically.'		
Remedial action: No recovery is needed. Retry periodically.		

Table 39-739 PoolManagerDHCPv6ClientStartFailed

Alarm	Attributes	Applicable major release
Name: PoolManagerDHCPv6ClientStartFailed (9594) Type: processingErrorAlarm Package: service. PoolManagerDHCPv6ClientStartFailed Raised on class: service.SubscriberInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerDHCPv6ClientStartFailed	Release: • N/A
Description: This notification is sent when a DHCPv6 client of the Pool Manager failed to start. [CAUSE] Failed to start a DHCPv6 client. [EFFECT] No pools can be requested for this ISA-BB. [RECOVERY] Perform a shutdown/no shutdown of the DHCPv6 client.		
Remedial action: Perform a shutdown/no shutdown of the DHCPv6 client.		

Table 39-740 PoolManagerNewPoolRequestFailed

Alarm	Attributes	Applicable major release
Name: PoolManagerNewPoolRequestFailed (9595) Type: processingErrorAlarm Package: service.PoolManagerNewPoolRequestFailed Raised on class: service.SubscriberInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerNewPoolRe-questFailed	Release: • N/A
Description: This notification is sent when sending a request for a new pool is failing. (For example, when a DHCPv6 server is unreachable.) [CAUSE] Failed to send a request for a new pool. [EFFECT] The ISA-BB may run out of free DHCPv6 addresses or SLAAC prefixes. [RECOVERY] No recovery is needed. Retry periodically.		
Remedial action: No recovery is needed. Retry periodically.		

Table 39-741 PoolManagerPoolTimeout

Alarm	Attributes	Applicable major release
Name: PoolManagerPoolTimeout (9037) Type: processingErrorAlarm Package: dhcp.PoolManagerPoolTimeout Raised on class: dhcp.Address6Pool	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerPoolTimeout	Release: • N/A
Description: This notification is sent when a pool is timing out unexpectedly. [CAUSE] Pool timed out unexpectedly. [EFFECT] The pool is removed from the ISA-BB together with all associated UEs. [RECOVERY] No recovery possible.		
Remedial action: No recovery possible.		

Table 39-742 PoolManagerPoolUsageLow

Alarm	Attributes	Applicable major release
Name: PoolManagerPoolUsageLow (9038) Type: processingErrorAlarm Package: dhcp.PoolManagerPoolUsageLow Raised on class: dhcp.Address6Pool	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PoolManagerPoolUsageLow	Release: • N/A
Description: This notification is sent when the usage of a pool drops below 1%. [CAUSE] Pool usage dropped below 1%. [EFFECT] The pool has become stale. [RECOVERY] Manually clear the pool.		
Remedial action: Manually clear the pool.		

Table 39-743 PostDiscoveryScriptExecutionFailed

Alarm	Attributes	Applicable major release
Name: PostDiscoveryScriptExecutionFailed (4868) Type: discoveryControlAlarm Package: netw.PostDiscoveryScriptExecutionFailed Raised on class: netw.NodeDiscoveryControl	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: scriptExecutionError	Release: • N/A
Description: The alarm is raised when the execution of the post discovery script failed. At this point, the NE is successfully discovered, only the auto configuration of the NE defined in the script failed. Manual intervention is required.		
Remedial action: The post discovery NE auto configuration script execution failed. run the script manually, or configure the NE manually. \nTo clear the Failed post discovery script execution status, click the "Clear" button on the Node Discovery Control configuration form: Administration->Discovery Manager->Managed State tab. Clearing the script execution status will also clear the associated alarm.		

Table 39-744 PostDiscoveryScriptNotExecuted

Alarm	Attributes	Applicable major release
Name: PostDiscoveryScriptNotExecuted (4869) Type: discoveryControlAlarm Package: netw.PostDiscoveryScriptNotExecuted Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resyncFailed	Release: • N/A
Description: The alarm is raised when the post discovery script is not executed. This is normally due to NE discovery failure. Manual intervention is required.		
Remedial action: The post discovery NE auto configuration script was not executed. Run the script manually, or configure the NE manually. \nThis is normally due to NE discovery failure. Fix the node resync issue associated with the PollerProblem alarm, unmanage and delete the node from the network, then rescan the discovery rule.		

Table 39-745 PowerSupplyACRectifierFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyACRectifierFailure (5181) Type: equipmentAlarm Package: equipment.PowerSupplyACRectifierFailure Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplACRectifierFaile-dorMissing	Release: • N/A
Description: This alarm is generated if any one of the AC rectifiers for a given power supply is in a failed state or is missing. When the alarm is raised during device discovery, one or both AC Rectifiers of the Power Supply Tray may be not equipped. When the alarm is raised while the device is in the managed state, one or both AC Rectifiers of the Power Supply Tray might be removed or they have a fault condition. The alarm clears when the status changes to OK.		
Remedial action: Ensure that the NE is properly connected to power. There is an increased risk of the power supply failing, causing insufficient power to the system. Please bring the AC rectifiers back online by equipping them properly. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-746 PowerSupplyVoltageAlarm

Alarm	Attributes	Applicable major release
Name: PowerSupplyVoltageAlarm (1129) Type: equipmentAlarm Package: equipment.PowerSupplyVoltageAlarm Raised on class: equipment.PowerSupply	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: powerSupplyFailure	Release: • N/A
Description: The alarm is raised when the power supply voltage alarm state changes to a value other than Normal.		
Remedial action: Check the status of the site power supply.		

Table 39-747 PowerSupplyWrongFanDir

Alarm	Attributes	Applicable major release
Name: PowerSupplyWrongFanDir (8166) Type: equipmentAlarm Package: equipment.PowerSupplyWrongFanDir Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyWrongFanDir	Release: • N/A
Description: This alarm is generated when the airflow direction of the power supply's fan is incorrect.		
Remedial action: To recover from this event, the customer is requested to replace the power supply with one that has the proper fan direction.		

Table 39-748 PppNcpFailure

Alarm	Attributes	Applicable major release
Name: PppNcpFailure (3689) Type: processingErrorAlarm Package: service.PppNcpFailure Raised on class: service.ServiceAccessPoint	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapAtmPppNcpFailure	Release: • N/A
Description: The alarm is raised when there is an NCP phase setup problem.		
Remedial action: This alarm indicates the NCP phase setup failed, thus IP protocol can not be configured for the user that attempted to set up the PPP session. Please verify NCP setup configuration.		

Table 39-749 PPPoASessionFailure

Alarm	Attributes	Applicable major release
Name: PPPoASessionFailure (3688) Type: processingErrorAlarm Package: service.PPPoASessionFailure Raised on class: service.AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapAtmPppSessionFailure	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot create a PPPoA Session.		
Remedial action: This alarm indicates the problem encountered by NE while trying to create a new PPPoA session. Please review the alarm's additional text to obtain information about the error condition. Possible problems include authentication failures, LCP or IPCP layer problems during the session establishment, or possible mis-configuration on the service interface or PPP policy.		

Table 39-750 PPPoESessionFailure

Alarm	Attributes	Applicable major release
Name: PPPoESessionFailure (2915) Type: processingErrorAlarm Package: service.PPPoESessionFailure Raised on class: service.ServiceAccessPoint	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: pppoeSessionFailed	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot create a PPPoE Session.		
Remedial action: This alarm indicates the problem encountered by NE while trying to create a new PPPoE session. Please review the alarm's additional text to obtain information about the error condition. Possible problems include authentication failures, LCP or IPCP layer problems during the session establishment, or possible mis-configuration on the service interface or PPP policy.		

Table 39-751 PrefixLimitExceeded

Alarm	Attributes	Applicable major release
Name: PrefixLimitExceeded (4) Type: ProtocolAlarm Package: bgp.PrefixLimitExceeded Raised on class: bgp.Peer	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: prefixLimitExceeded	Release: • N/A
Description: The alarm is raised when a BGP instance learns the maximum number of peer routes.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of peer routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-752 PrefixLimitNearing

Alarm	Attributes	Applicable major release
Name: PrefixLimitNearing (3) Type: ProtocolAlarm Package: bgp.PrefixLimitNearing Raised on class: bgp.Peer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: prefixLimitNearing	Release: • N/A
Description: The alarm is raised when a BGP instance exceeds the threshold percentage of the configured maximum.		
Remedial action: Informational. The threshold configured should be revisited to ensure that it is not set to low given the number of peer routes that are being received. If the threshold is set close to the maximum number of routes supported by the NE then it is probable that there is an issue with another NE in the network. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-753 PrefixUnreachable

Alarm	Attributes	Applicable major release
Name: PrefixUnreachable (8428) Type: virtualSwitchAlarm Package: dctr.PrefixUnreachable Raised on class: dctr.AbstractVirtualSwitchGlobal	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrefixDown	Release: • N/A
Description: The alarm is raised when the Prefix is unreachable i.e. all the advertising routers are down.		
Remedial action: This alarm can be cleared when the IGP or BGP Prefix for the Virtual Switch is reachable.		

Table 39-754 PrimaryDatabaseDown

Alarm	Attributes	Applicable major release
Name: PrimaryDatabaseDown (751) Type: databaseAlarm Package: db.PrimaryDatabaseDown Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: primaryDatabaseDown	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM database is down for at least one poll. The alarm is not persisted in the database or stored in the alarm history; when the database returns to service, the PrimaryDatabaseWasDown alarm is raised.		
Remedial action: Informational - verify connectivity to the primary database server		

Table 39-755 PrimaryDatabaseWasDown

Alarm	Attributes	Applicable major release
Name: PrimaryDatabaseWasDown (254) Type: databaseAlarm Package: db.PrimaryDatabaseWasDown Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: primaryDatabaseWasDown	Release: • N/A
Description: The alarm is raised when the primary database returns to service after being unavailable for at least one poll.		
Remedial action: Informational - no corrective action required.		

Table 39-756 PrimaryVirtualServicesControllerFailed

Alarm	Attributes	Applicable major release
Name: PrimaryVirtualServicesControllerFailed (8429) Type: virtualSwitchAlarm Package: dctr.PrimaryVirtualServicesControllerFailed Raised on class: dctr.AbstractVirtualSwitchGlobal	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PrimaryControllerFailOver	Release: • N/A
Description: The alarm is raised when communication between the virtual switch to the primary controller has failed.		
Remedial action: This alarm can be cleared when primary virtual switch is operationally up.		

Table 39-757 ProbeFailedAlarm (mpls)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: mpls.ProbeFailedAlarm Raised on class: mpls.Lsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		

Table 39-757 ProbeFailedAlarm (mpls) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-758 ProbeFailedAlarm (mirror)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: mirror.ProbeFailedAlarm Raised on class: mirror.Mirror	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-759 ProbeFailedAlarm (ethernetoam)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: ethernetoam.ProbeFailedAlarm Raised on class: ethernetoam.MaintAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-760 ProbeFailedAlarm (vprn)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: vprn.ProbeFailedAlarm Raised on class: vprn.Vprn	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-761 ProbeFailedAlarm (svt)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: svt.ProbeFailedAlarm Raised on class: svt.Tunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-762 ProbeFailedAlarm (rtr)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: rtr.ProbeFailedAlarm Raised on class: rtr.VirtualRouter	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-763 ProbeFailedAlarm (mplstp)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: mplstp.ProbeFailedAlarm Raised on class: mplstp.TPLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-764 ProbeFailedAlarm (monpath)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: monpath.ProbeFailedAlarm Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-764 ProbeFailedAlarm (monpath) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-765 ProbeFailedAlarm (lte)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: lte.ProbeFailedAlarm Raised on class: lte.EPSPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when ProbeFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-766 ProbeFailedAlarm (service)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: service.ProbeFailedAlarm Raised on class: service.SpokeConnector	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when ProbeFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-767 ProbeFailedAlarm (netw)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: netw.ProbeFailedAlarm Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-768 ProbeFailedAlarm (pim)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: pim.ProbeFailedAlarm Raised on class: pim.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-769 ProbeFailedAlarm (bgp)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: bgp.ProbeFailedAlarm Raised on class: bgp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-770 ProbeFailedAlarm (ldp)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: ldp.ProbeFailedAlarm Raised on class: ldp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-771 ProbeFailedAlarm (lteservice)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: lteservice.ProbeFailedAlarm Raised on class: lteservice.MobileService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-771 ProbeFailedAlarm (lteservice) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-772 ProbeFailedAlarm (vll)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: vll.ProbeFailedAlarm Raised on class: vll.Vll	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-773 ProbeFailedAlarm (vpls)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: vpls.ProbeFailedAlarm Raised on class: vpls.AbstractVpls	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-774 ProbeFailedAlarm (atm)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm (3707) Type: oamAlarm Package: atm.ProbeFailedAlarm Raised on class: atm.PvcConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-775 ProbeFailedAlarm2 (svt)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: svt.ProbeFailedAlarm2 Raised on class: svt.SdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-776 ProbeFailedAlarm2 (ethernetoam)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: ethernetoam.ProbeFailedAlarm2 Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-777 ProbeFailedAlarm2 (service)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: service.ProbeFailedAlarm2 Raised on class: service.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when ProbeFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-778 ProbeFailedAlarm2 (mpls)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: mpls.ProbeFailedAlarm2 Raised on class: mpls.P2MPDynamicLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-778 ProbeFailedAlarm2 (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-779 ProbeFailedAlarm2 (atm)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: atm.ProbeFailedAlarm2 Raised on class: atm.VPConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-780 ProbeFailedAlarm2 (lte)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: lte.ProbeFailedAlarm2 Raised on class: lte.EPSPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when ProbeFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-781 ProbeFailedAlarm2 (rtr)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm2 (3738) Type: oamAlarm Package: rtr.ProbeFailedAlarm2 Raised on class: rtr.LDPTunnelInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-782 ProbeFailedAlarm3 (service)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm3 (3885) Type: oamAlarm Package: service.ProbeFailedAlarm3 Raised on class: service.CompositeService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-783 ProbeFailedAlarm3 (mpls)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm3 (3885) Type: oamAlarm Package: mpls.ProbeFailedAlarm3 Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-784 ProbeFailedAlarm3 (svt)

Alarm	Attributes	Applicable major release
Name: ProbeFailedAlarm3 (3885) Type: oamAlarm Package: svt.ProbeFailedAlarm3 Raised on class: svt.SpokeSdpFec	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports a probe failure.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-785 ProbeFailureAlarm

Alarm	Attributes	Applicable major release
Name: ProbeFailureAlarm (3902) Type: oamAlarm Package: sas.ProbeFailureAlarm Raised on class: sas.Test	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-785 ProbeFailureAlarm (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when a probe failure trap is received from the node.		
Remedial action: Fix network connections issues.		

Table 39-786 ProxyArpDupDetect

Alarm	Attributes	Applicable major release
Name: ProxyArpDupDetect (9604) Type: configurationAlarm Package: vpls.ProxyArpDupDetect Raised on class: vpls.ProxyArpEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: macAddrMisconfigured	Release: • N/A
Description: This alarm is generated when duplicate detection criteria is met when a new mac address overwrites the existing mac address for the proxy arp entry. A traffic disruption may occur if both systems are active. Identify and correct configuration of one of the systems.		
Remedial action: Identify and correct configuration of mac address of one of the systems.		

Table 39-787 ProxyArpSvcHiUsgSet

Alarm	Attributes	Applicable major release
Name: ProxyArpSvcHiUsgSet (9605) Type: processingErrorAlarm Package: vpls.ProxyArpSvcHiUsgSet Raised on class: vpls.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proxyArpSvcHiUsgSet	Release: • N/A
Description: This alarm is generated when the number of proxy ARP entries in a VPLS service exceeds 95% of the per-service limit.		
Remedial action: Informational - the number of proxy ARP entries in a VPLS service exceeds 95% of the per-service limit		

Table 39-788 ProxyArpSysHiUsgSet

Alarm	Attributes	Applicable major release
Name: ProxyArpSysHiUsgSet (9580) Type: processingErrorAlarm Package: netw.ProxyArpSysHiUsgSet Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proxyArpSysHiUsgSet	Release: • N/A
Description: This alarm is generated when the number of proxy ARP entries in the system exceeds 95% of the system limit.		
Remedial action: Informational - the number of proxy ARP entries in the system exceeds 95% of the system limit		

Table 39-789 ProxyDown

Alarm	Attributes	Applicable major release
Name: ProxyDown (1959) Type: communicationsAlarm Package: db.ProxyDown Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when proxy server communication fails.		
Remedial action: The Oracle Proxy runs on the 5620 SAM database workstations. To determine if the Oracle Proxy is running login to the database workstation, open a terminal and run the command ps -eaf | grep oracleproxy. If there is no oracleproxy process running, start the process using /etc/rc3.d/S965620SAMOracleProxyWrapper start.		

Table 39-790 ProxyNdDupDetect

Alarm	Attributes	Applicable major release
Name: ProxyNdDupDetect (9606) Type: configurationAlarm Package: vpls.ProxyNdDupDetect Raised on class: vpls.ProxyNdEntry	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: macAddrMisconfigured	Release: • N/A
Description: This alarm is generated when duplicate detection criteria is met when a new mac address overwrites the existing mac address for the proxy ND entry. A traffic disruption may occur if both sytems are active. Identify and correct configuration of one of the systems.		
Remedial action: Identify and correct configuration of mac address of one of the systems.		

Table 39-791 ProxyNdSvcHiUsgSet

Alarm	Attributes	Applicable major release
Name: ProxyNdSvcHiUsgSet (9607) Type: processingErrorAlarm Package: vpls.ProxyNdSvcHiUsgSet Raised on class: vpls.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proxyNdSvcHiUsgSet	Release: • N/A
Description: This alarm is generated when the number of proxy ND entries in a VPLS service exceeds 95% of the per-service limit.		
Remedial action: Informational - the number of proxy ND entries in a VPLS service exceeds 95% of the per-service limit		

Table 39-792 ProxyNdSysHiUsgSet

Alarm	Attributes	Applicable major release
Name: ProxyNdSysHiUsgSet (9581) Type: processingErrorAlarm Package: netw.ProxyNdSysHiUsgSet Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: proxyNdSysHiUsgSet	Release: • N/A

Table 39-792 ProxyNdSysHiUsgSet (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is generated when the number of proxy ND entries in the system exceeds 95% of the system limit.		
Remedial action: Informational - the number of proxy ND entries in the system exceeds 95% of the system limit		

Table 39-793 PTPCardNotSupportedAlarm

Alarm	Attributes	Applicable major release
Name: PTPCardNotSupportedAlarm (3603) Type: equipmentAlarm Package: ptp.PTPCardNotSupportedAlarm Raised on class: ptp.IEEEPTPClock	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPCardNotSupported	Release: • N/A
Description: The alarm is raised when the Precision Timing Protocol (PTP) is enabled on a card that does not support clock recovery.		
Remedial action: Please enable PTP on CPM which supports OCX0 oscillator type		

Table 39-794 PTPClockRecoveryStateAlarm

Alarm	Attributes	Applicable major release
Name: PTPClockRecoveryStateAlarm (3605) Type: communicationsAlarm Package: ptp.PTPClockRecoveryStateAlarm Raised on class: ptp.IEEEPTPClock	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PTPClockRecoveryStat-eChange	Release: • N/A
Description: The alarm is raised when the aluPtpClockRecoveryState changes for an IEEE 1588 Precision Timing Protocol (PTP) clock.		
Remedial action: Informational		

Table 39-795 PTPMasterChangeAlarm

Alarm	Attributes	Applicable major release
Name: PTPMasterChangeAlarm (3606) Type: communicationsAlarm Package: ptp.PTPMasterChangeAlarm Raised on class: ptp.IEEEPTPClock	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PTPMasterChange	Release: • N/A
Description: The alarm is raised when there is a change in the synchronization source for a Precision Timing Protocol (PTP) clock.		
Remedial action: Informational		

Table 39-796 PTPOutOfResourcesAlarm

Alarm	Attributes	Applicable major release
Name: PTPOutOfResourcesAlarm (3607) Type: equipmentAlarm Package: ptp.PTPOutOfResourcesAlarm Raised on class: ptp.IEEEPTPClock	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPOutOfResources	Release: • N/A
Description: The alarm is raised when the Precision Timing Protocol (PTP) process on the card is out of resources. This may occur in either of two situations: 1. The number of PTP peers exceeds the system limit. 2. The total unicast packet rate negotiated with all PTP peers reaches the maximum packet rate supported by the system.		
Remedial action: Informational		

Table 39-797 PTPPortDSPortStateAlarm

Alarm	Attributes	Applicable major release
Name: PTPPortDSPortStateAlarm (3610) Type: communicationsAlarm Package: ptp.PTPPortDSPortStateAlarm Raised on class: ptp.IEEEPTPPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPPortDSPortState	Release: • N/A
Description: The alarm is raised when the aluPtpPortDSPortState changes for an IEEE 1588 Precision Timing Protocol (PTP) port.		
Remedial action: Informational.		

Table 39-798 PTPQualityLevelChangedAlarm

Alarm	Attributes	Applicable major release
Name: PTPQualityLevelChangedAlarm (3612) Type: communicationsAlarm Package: sonet.PTPQualityLevelChangedAlarm Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: PTPQualityLevelChanged	Release: • N/A
Description: The alarm is raised when there is a change of the received quality level on the Precision Timing Protocol (PTP).		
Remedial action: Informational only.		

Table 39-799 PTPReferenceLossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: PTPReferenceLossOfSignal (3613) Type: communicationsAlarm Package: equipment.PTPReferenceLossOfSignal Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceLossOfSignal	Release: • N/A
Description: The alarm is raised on the Standby CPM when the PTP reference on an NE is not qualified due to Loss of Signal.		

Table 39-799 PTPReferenceLossOfSignal (equipment) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 39-800 PTPReferenceOutOfFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfFrequency (3614) Type: communicationsAlarm Package: equipment.PTPReferenceOutOfFrequency Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfFrequency	Release: • N/A
Description: The alarm is raised on the Standby CPM when the PTP Reference on an NE is not qualified due to Out of frequency.		
Remedial action: Make sure that frequency configured for Reference One is correct.		

Table 39-801 PTPReferenceOutOfPollInRange (equipment)

Alarm	Attributes	Applicable major release
Name: PTPReferenceOutOfPollInRange (3615) Type: communicationsAlarm Package: equipment.PTPReferenceOutOfPollInRange Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PTPReferenceOutOfPollInRange	Release: • N/A
Description: The alarm is raised on the Standby CPM when the PTP Reference on an NE is not qualified state due to Out of poll in range.		
Remedial action: If there is packet flow, the PTP slave clock is in it's initial acquiring states where the sync-if-timing reference does not qualify just wait.		

Table 39-802 PurgeFilesToFreeDiskSpace

Alarm	Attributes	Applicable major release
Name: PurgeFilesToFreeDiskSpace (1937) Type: serverAlarm Package: server.PurgeFilesToFreeDiskSpace Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the 5620 SAM server deletes files in order to free disk space.		
Remedial action: Informational - this is a generic error if SAM Server free disk space is below acceptable levels and files must be purged to free the disk space. The additional text field of the alarm will provide more details of the specific problem. Reduce the disk space by purging the files using the commands available in the SAM GUI. It may be necessary to add additional disk space to the system to resolve the problem.		

Table 39-803 QChipBufferMemoryEvent

Alarm	Attributes	Applicable major release
Name: QChipBufferMemoryEvent (4990) Type: hardwareAnomaly Package: equipment.QChipBufferMemoryEvent Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bufMemoryError	Release: • N/A
Description: The alarm is raised when a Q-chip experiences an occurrence of a buffer memory error on IOM or CPM.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-804 QChipIntMemoryEvent

Alarm	Attributes	Applicable major release
Name: QChipIntMemoryEvent (4993) Type: hardwareAnomaly Package: equipment.QChipIntMemoryEvent Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: intMemoryError	Release: • N/A
Description: The alarm is raised when a Q-chip experiences an occurrence of an internal memory error on IOM or CPM.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-805 QChipStatsMemoryEvent

Alarm	Attributes	Applicable major release
Name: QChipStatsMemoryEvent (4994) Type: hardwareAnomaly Package: equipment.QChipStatsMemoryEvent Raised on class: equipment.Card	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: statsMemoryError	Release: • N/A
Description: The alarm is raised when a Q-chip experiences an occurrence of a statistics memory error on IOM or CPM.		
Remedial action: A fault has been detected in the hardware if the problem persists please contact your Nokia support representative for assistance.		

Table 39-806 QueryVerMismatch

Alarm	Attributes	Applicable major release
Name: QueryVerMismatch (159) Type: configurationAlarm Package: igmp.QueryVerMismatch Raised on class: igmp.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: InvalidVersionofQueryMes-sageReceived	Release: • N/A

Table 39-806 QueryVerMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an interface configured for IGMPv3 receives a query message for an earlier IGMP version. The interface subsequently enters an IGMP mode that is compatible with the earlier version. The alarm information includes the IGMP version on the interface and the IGMP version of the received query.		
Remedial action: Informational - no corrective action required.		

Table 39-807 RadAcctOnOngoing

Alarm	Attributes	Applicable major release
Name: RadAcctOnOngoing (4971) Type: radiusAccountingPolicyAlarm Package: aaa.RadAcctOnOngoing Raised on class: aaa.RadiusServerPolicy	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: TooManyUnacknowledgedRadiusAccountingOnMessages Applicable probable causes: • TooManyUnacknowledgedRadiusAccountingOnMessages • MisconfiguredPolicy • RadiusServerUnreachable • MissingClientInformation	Release: • N/A
Description: The alarm is raised each time when the RADIUS client has sent 10 RADIUS Accounting-On messages without receiving any acknowledgement from the RADIUS server.		
Remedial action: Ensure that:\n1.The RADIUS server is up and running.\n2.The RADIUS server policy configuration is correct.\n\nPlease note that this system will keep on retrying indefinitely until it receives an acknowledgement from the RADIUS server.		

Table 39-808 RadioEncryptionMismatch (mwa)

Alarm	Attributes	Applicable major release
Name: RadioEncryptionMismatch (8969) Type: communicationsAlarm Package: mwa.RadioEncryptionMismatch Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RadioEncryptionMismatch	Release: • N/A
Description: The alarm is raised when a MPT detects a radio encryption mismatch.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-809 RadioHop15TCA

Alarm	Attributes	Applicable major release
Name: RadioHop15TCA (4835) Type: communicationsAlarm Package: mwa.RadioHop15TCA Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ThresholdCrossed	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio hop 15 minutes TCA		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-810 RadioHop15UAT

Alarm	Attributes	Applicable major release
Name: RadioHop15UAT (4836) Type: communicationsAlarm Package: mwa.RadioHop15UAT Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnavailableTime	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio hop 15 minutes UAT		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-811 RadioHop24TCA

Alarm	Attributes	Applicable major release
Name: RadioHop24TCA (4837) Type: communicationsAlarm Package: mwa.RadioHop24TCA Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ThresholdCrossed	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio hop 24 Hours TCA		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-812 RadioHop24UAT

Alarm	Attributes	Applicable major release
Name: RadioHop24UAT (4838) Type: communicationsAlarm Package: mwa.RadioHop24UAT Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnavailableTime	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio hop 24 Hours UAT		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-813 RadioLink15TCA

Alarm	Attributes	Applicable major release
Name: RadioLink15TCA (4839) Type: communicationsAlarm Package: mwa.RadioLink15TCA Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ThresholdCrossed	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio Link 15 minutes TCA		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-814 RadioLink15UAT

Alarm	Attributes	Applicable major release
Name: RadioLink15UAT (4840) Type: communicationsAlarm Package: mwa.RadioLink15UAT Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnavailableTime	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio Link 15 minutes UAT		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-815 RadioLink24TCA

Alarm	Attributes	Applicable major release
Name: RadioLink24TCA (4841) Type: communicationsAlarm Package: mwa.RadioLink24TCA Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ThresholdCrossed	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio Link 24 Hours TCA		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-816 RadioLink24UAT

Alarm	Attributes	Applicable major release
Name: RadioLink24UAT (4842) Type: communicationsAlarm Package: mwa.RadioLink24UAT Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnavailableTime	Release: • N/A
Description: The alarm is raised when a MPT detects a threshold crossing - Radio Link 24 Hours UAT		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-817 RadioLoopProblemCh1

Alarm	Attributes	Applicable major release
Name: RadioLoopProblemCh1 (4843) Type: communicationsAlarm Package: mwa.RadioLoopProblemCh1 Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoopProblem	Release: • N/A
Description: The alarm is raised when a MPT detects a ATPC/ACM Loop problem - CH1 Radio Loop Problem		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-818 RadioLoopProblemChx

Alarm	Attributes	Applicable major release
Name: RadioLoopProblemChx (4844) Type: communicationsAlarm Package: mwa.RadioLoopProblemChx Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LoopProblem	Release: • N/A
Description: The alarm is raised when a MPT detects a ATPC/ACM Loop problem - CHX Radio Loop Problem		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-819 RadioRdi

Alarm	Attributes	Applicable major release
Name: RadioRdi (4846) Type: communicationsAlarm Package: mwa.RadioRdi Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: Rdi	Release: • N/A
Description: The alarm is raised when a microwave radio device receives a remote defect indication from the far end microwave radio.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-820 RadioSwPackageMissing

Alarm	Attributes	Applicable major release
Name: RadioSwPackageMissing (4848) Type: integrityViolation Package: mwa.RadioSwPackageMissing Raised on class: mwa.PortTermination	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SwPackageMissing	Release: • N/A
Description: The alarm is raised when a valid microwave radio software package is not present at startup.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-821 RadiusInsertedFltrEntryDropped

Alarm	Attributes	Applicable major release
Name: RadiusInsertedFltrEntryDropped (1152) Type: configurationAlarm Package: aclfilter.RadiusInsertedFltrEntryDropped Raised on class: aclfilter.FilterDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: FilterEntryDropped	Release: • N/A
Description: The alarm is raised when a request to insert a filter entry is not successful for a RADIUS application.		
Remedial action: A Configuration error has occurred. The request to insert a filter entry was not successful for Radius application. Check the configuration filter entry.		

Table 39-822 RadiusInsertSpaceThresholdAlarm

Alarm	Attributes	Applicable major release
Name: RadiusInsertSpaceThresholdAlarm (1151) Type: configurationAlarm Package: aclfilter.RadiusInsertSpaceThresholdAlarm Raised on class: aclfilter.FilterDefinition	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UtilizationExceedConfigured-Limit	Release: • N/A
Description: The alarm is raised when the utilization of a filter entry range that is reserved for filter entry insertion increases to the configured maximum value for a RADIUS application insert range.		
Remedial action: The filter entry range reserved for filter entry insertion has increased to the configured high watermark for Radius application. Make an adjusted to the watermarks or to the filter.		

Table 39-823 radiusServerOverloaded (subscrauth)

Alarm	Attributes	Applicable major release
Name: radiusServerOverloaded (3913) Type: communicationsAlarm Package: subscrauth.radiusServerOverloaded Raised on class: subscrauth.RadiusEntry	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusServerRequestLimi-tReached	Release: • N/A
Description: The alarm is raised when the RADIUS server is overloaded.		
Raising condition: (('Operational State' EQUAL 'Over Loaded'))		
Clearing condition: (('Operational State' NOT EQUAL 'Over Loaded'))		
Remedial action: Verify the RADIUS server is properly configured to process pending authentication requests at the desired rate and ensure that this rate matches the authentication request limit defined for this RADIUS server on the network element.		

Table 39-824 RadRouteDownloadFailed

Alarm	Attributes	Applicable major release
Name: RadRouteDownloadFailed (4418) Type: communicationsAlarm Package: aaa.RadRouteDownloadFailed Raised on class: aaa.RouteDownloadPolicy	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when a RADIUS route-download process fails.		
Remedial action: Ensure that:\n1.The routes defined in the RADIUS Server have a valid syntax.\n2.The number of downloaded routes is less than the maximum.\n3.There are no issues affecting the node's ability to populate the routes into the routing table.		

Table 39-825 RDI (mpr)

Alarm	Attributes	Applicable major release
Name: RDI (806) Type: communicationsAlarm Package: mpr.RDI Raised on class: mpr.IMALink	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteDefectIndication	Release: • N/A
Description: The alarm is raised when a Remote Defect Indication signal is detected on an ASAP MDA.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-826 RDICh1

Alarm	Attributes	Applicable major release
Name: RDICh1 (4833) Type: communicationsAlarm Package: mwa.RDICh1 Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteDefectIndication	Release: • N/A
Description: The alarm is raised when a MPT receives a remote MPT CH1 remote defect indication		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-827 RDIChx

Alarm	Attributes	Applicable major release
Name: RDIChx (4834) Type: communicationsAlarm Package: mwa.RDIChx Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteDefectIndication	Release: • N/A
Description: The alarm is raised when a MPT receives a remote MPT CHX remote defect indication		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-828 RealignmentOfDatabase

Alarm	Attributes	Applicable major release
Name: RealignmentOfDatabase (613) Type: configurationAlarm Package: db.RealignmentOfDatabase Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: databaseRealignment	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM main server realigns itself with the preferred database by performing a database switchover to connect to the primary database.		
Remedial action: Informational - no corrective action required.		

Table 39-829 RealignmentOfDatabaseFailed

Alarm	Attributes	Applicable major release
Name: RealignmentOfDatabaseFailed (614) Type: configurationAlarm Package: db.RealignmentOfDatabaseFailed Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: databaseRealignmentFailed	Release: • N/A
Description: The alarm is raised when a database switchover to realign the primary main server and primary database fails. The primary main server is not connected to the preferred database.		
Remedial action: The additional text field of the alarm will provide more details as will the EmsServer.log. Possible causes include a HW failure on the platform hosting the database function, loss of network connectivity between the primary and standby database platforms. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-830 ReceivedHigherBridgePriority

Alarm	Attributes	Applicable major release
Name: ReceivedHigherBridgePriority (504) Type: SdpBindingAlarm Package: l2fwd.ReceivedHigherBridgePriority Raised on class: l2fwd.CircuitStp	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: customerDeviceMisconfigured	Release: • N/A
Description: The alarm is raised when a customer NE is configured with a bridge priority of zero. The SDP binding that connects to the customer device is subsequently blocked.		
Remedial action: Remove the customer's device or reconfigure the customer's bridge priority with value greater than zero.		

Table 39-831 RedAlarmThresholdReached

Alarm	Attributes	Applicable major release
Name: RedAlarmThresholdReached (241) Type: communicationsAlarm Package: netw.RedAlarmThresholdReached Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyAlarms	Release: • N/A
Description: The alarm is raised when the number of outstanding 5620 SAM alarms reaches the critical threshold. When this happens, the 5620 SAM discards alarms to keep the number below the threshold.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

Table 39-832 RedundancySwitchover

Alarm	Attributes	Applicable major release
Name: RedundancySwitchover (181) Type: equipmentAlarm Package: netw.RedundancySwitchover Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: CPMSwitchover	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server receives a CPMSwitchover trap from an NE, which indicates that the standby CPM detects an active CPM failure and is preparing to take over as the new active CPM.		
Remedial action: Informational.		

Table 39-833 RedundantIfMismatch

Alarm	Attributes	Applicable major release
Name: RedundantIfMismatch (419) Type: configurationAlarm Package: srrp.RedundantIfMismatch Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: redundantIfNotProperlyPaired	Release: • N/A
Description: The alarm is raised when the local and remote redundant interfaces are not correctly paired.		
Remedial action: Reconfigure the redundant interfaces for the peer SRRP instances so that they match each other.		

Table 39-834 RedundantRadioLink

Alarm	Attributes	Applicable major release
Name: RedundantRadioLink (1081) Type: configurationAlarm Package: netw.RedundantRadioLink Raised on class: netw.RadioPhysicalLink	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: redundantRadioLinkConfig-ured	Release: • N/A

Table 39-834 RedundantRadioLink (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a radio link is discovered between two nodes when there is already a physical link(s) between the same nodes.		
Remedial action: Informational-this alarm indicates that there is another radio link between the nodes involved.		

Table 39-835 ReferenceOneLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceOneLossOfSignal (1953) Type: communicationsAlarm Package: sonet.ReferenceOneLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneLossOfSignal	Release: • N/A
Description: The alarm is raised when the Timing Reference One on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to Reference One is properly configured.		

Table 39-836 ReferenceOneLossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceOneLossOfSignal (1953) Type: communicationsAlarm Package: equipment.ReferenceOneLossOfSignal Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneLossOfSignal	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference One on an NE is not qualified due to Loss of Signal.		
Remedial action: Make sure that peer connected to Reference One is properly configured.		

Table 39-837 ReferenceOneOutOfFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceOneOutOfFrequency (1954) Type: communicationsAlarm Package: equipment.ReferenceOneOutOfFrequency Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneOutOfFrequency	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference One on an NE is not qualified due to Out of frequency.		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 39-838 ReferenceOneOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceOneOutOfFrequency (1954) Type: communicationsAlarm Package: sonet.ReferenceOneOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneOutOfFrequency	Release: • N/A
Description: The alarm is raised when the Timing Reference One on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Check the communication path is up between the local PTP slave clock and its selected master		

Table 39-839 ReferenceOneOutOfPollInRange (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceOneOutOfPollInRange (1955) Type: communicationsAlarm Package: equipment.ReferenceOneOutOfPollInRange Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneOutOfPollInRange	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference One on an NE is not qualified due to Out of poll in range.		
Remedial action: Check the timing reference is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 39-840 ReferenceOneOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceOneOutOfPollInRange (1955) Type: communicationsAlarm Package: sonet.ReferenceOneOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceOneOutOfPollInRange	Release: • N/A
Description: The alarm is raised when the Timing Reference One on an NE is not qualified due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the timing reference is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 39-841 ReferenceTwoLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoLossOfSignal (1956) Type: communicationsAlarm Package: sonet.ReferenceTwoLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoLossOfSignal	Release: • N/A
Description: The alarm is raised when the Timing Reference Two on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to Reference Two is properly configured.		

Table 39-842 ReferenceTwoLossOfSignal (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoLossOfSignal (1956) Type: communicationsAlarm Package: equipment.ReferenceTwoLossOfSignal Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoLossOfSignal	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference Two on an NE is not qualified due to Loss of Signal.		
Remedial action: Make sure that peer connected to Reference Two is properly configured.		

Table 39-843 ReferenceTwoOutOfFrequency (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoOutOfFrequency (1957) Type: communicationsAlarm Package: equipment.ReferenceTwoOutOfFrequency Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoOutOfFrequency	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference Two on an NE is not qualified due to Out of frequency.		
Remedial action: Make sure that frequency configured for Reference Two is correct.		

Table 39-844 ReferenceTwoOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoOutOfFrequency (1957) Type: communicationsAlarm Package: sonet.ReferenceTwoOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoOutOfFrequency	Release: • N/A
Description: The alarm is raised when the Timing Reference Two on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for Reference Two is correct.		

Table 39-845 ReferenceTwoOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoOutOfPollInRange (1958) Type: communicationsAlarm Package: sonet.ReferenceTwoOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoOutOfPollInRange	Release: • N/A
Description: The alarm is raised when the Timing Reference Two on an NE is not qualified due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the timing reference is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 39-846 ReferenceTwoOutOfPollInRange (equipment)

Alarm	Attributes	Applicable major release
Name: ReferenceTwoOutOfPollInRange (1958) Type: communicationsAlarm Package: equipment.ReferenceTwoOutOfPollInRange Raised on class: equipment.ProcessorCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReferenceTwoOutOfPollInRange	Release: • N/A
Description: The alarm is raised on the Standby CPM when the Timing Reference Two on an NE is not qualified due to Out of poll in range.		
Remedial action: Check the timing reference is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary.		

Table 39-847 ReinstantiateStandbyDatabase

Alarm	Attributes	Applicable major release
Name: ReinstantiateStandbyDatabase (252) Type: configurationAlarm Package: db.ReinstantiateStandbyDatabase Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: reinstantiateStandbyDatabase	Release: • N/A
Description: The alarm is raised when a standby database reinstantiation occurs.		
Remedial action: Informational - no corrective action required.		

Table 39-848 ReinstantiateStandbyDatabaseFailed

Alarm	Attributes	Applicable major release
Name: ReinstantiateStandbyDatabaseFailed (253) Type: configurationAlarm Package: db.ReinstantiateStandbyDatabaseFailed Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: reinstantiateStandbyDatabaseFailed	Release: • N/A
Description: The alarm is raised when a standby database reinstantiation fails.		
Remedial action: The additional text field of the alarm will provide more details as will the EmsServer.log. Possible causes include a HW failure on the platform hosting the database function, loss of network connectivity between the primary and standby database platforms. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-849 RemoteNEFailure

Alarm	Attributes	Applicable major release
Name: RemoteNEFailure (1173) Type: equipmentAlarm Package: equipment.RemoteNEFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: remoteNEFailure	Release: • N/A
Description: The alarm is raised when a remote NE failure is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-850 ReplicationLmtExceeded

Alarm	Attributes	Applicable major release
Name: ReplicationLmtExceeded (3968) Type: resourceAlarm Package: equipment.ReplicationLmtExceeded Raised on class: equipment.BaseCard	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: resourceLimitReached	Release: • N/A

Table 39-850 ReplicationLmtExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IOM fails to program an OIF for an (S,G) record because the replication limit for that (S,G) on that IOM has been reached. The replication limit per (S,G) entry on an IOM is currently 127.		
Remedial action: Informational - no corrective action required		

Table 39-851 ReservedRouteTargetMismatch

Alarm	Attributes	Applicable major release
Name: ReservedRouteTargetMismatch (6446) Type: configurationAlarm Package: l3fwd.ReservedRouteTargetMismatch Raised on class: l3fwd.ServiceSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: reservedRouteTargetChanged	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects a pre-assigned route target on this VPRN has been modified. The alarm information includes the source, i.e., import or export, and the conflict reserved VPRN RT entry distinguished name.		
Remedial action: A configuration error has occurred which should be corrected. This VPRN's route target has been modified from its pre-reserved value defined in the Reserved VPRN Route Target Table.		

Table 39-852 ResiliencySapDeleted

Alarm	Attributes	Applicable major release
Name: ResiliencySapDeleted (688) Type: resiliencyAlarm Package: resiliency.ResiliencySapDeleted Raised on class: resiliency.HsdpaResiliency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resiliencySapDeleted	Release: • N/A
Description: The alarm is raised when a SAP that is used for resiliency is deleted.		
Remedial action: Informational.		

Table 39-853 ResiliencyServiceSwitch

Alarm	Attributes	Applicable major release
Name: ResiliencyServiceSwitch (689) Type: resiliencyAlarm Package: resiliency.ResiliencyServiceSwitch Raised on class: resiliency.HsdpaResiliency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: secondaryServiceSiteActive	Release: • N/A
Description: The alarm is raised when a secondary service becomes active.		
Remedial action: Informational.		

Table 39-854 ResiliencySiteDeleted

Alarm	Attributes	Applicable major release
Name: ResiliencySiteDeleted (690) Type: resiliencyAlarm Package: resiliency.ResiliencySiteDeleted Raised on class: resiliency.HsdpaResiliency	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: secondaryServiceSiteDeleted	Release: • N/A
Description: The alarm is raised when a secondary service site is deleted.		
Remedial action: Informational.		

Table 39-855 restoreFailureAlarm

Alarm	Attributes	Applicable major release
Name: restoreFailureAlarm (535) Type: softwareAlarm Package: sw.restoreFailureAlarm Raised on class: sw.SoftwareControlModule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: restoreFailureAlarm	Release: • N/A
Description: The alarm is raised when the software restore process on an NE fails.		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 39-856 RevertiveMisMatch

Alarm	Attributes	Applicable major release
Name: RevertiveMisMatch (4899) Type: pathAlarm Package: mplstp.RevertiveMisMatch Raised on class: mplstp.PathMep	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RevertiveMisMatch	Release: • N/A
Description: This alarm is generated when an MPLS-TP LSP revertive mode mismatch is detected on the protection MEP. The revertive mode must match on the local node and the far-end node.		
Remedial action: This alarm is generated when an MPLS-TP LSP revertive mode mismatch is detected on the protection MEP. The revertive mode must match on the local node and the far-end node.		

Table 39-857 RFSwitchFail (mwa)

Alarm	Attributes	Applicable major release
Name: RFSwitchFail (5425) Type: equipmentAlarm Package: mwa.RFSwitchFail Raised on class: mwa.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RFSwitchFailure	Release: • N/A

Table 39-857 RFSwitchFail (mwa) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MPT detects a Radio Frame Switch Failure.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-858 RingAuditProblem

Alarm	Attributes	Applicable major release
Name: RingAuditProblem (4995) Type: configurationAlarm Package: ethring.RingAuditProblem Raised on class: ethring.Ring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: invalidConfiguation	Release: • N/A
Description: The alarm is raised when the Ring Audit has detected a problem.		
Remedial action: A configuration error has been made which must be corrected. Please see the additional test for more details.		

Table 39-859 RipAuthenticationFailure

Alarm	Attributes	Applicable major release
Name: RipAuthenticationFailure (70) Type: authenticationAlarm Package: rip.RipAuthenticationFailure Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authFailure	Release: • N/A
Description: The alarm is raised when a peer authentication failure occurs. The alarm information includes the peer address.		
Remedial action: Informational - please check that RIP neighbor is sending the RIPv2 packet with the matching authentication key with this router.		

Table 39-860 RipAuthenticationMismatch

Alarm	Attributes	Applicable major release
Name: RipAuthenticationMismatch (71) Type: authenticationAlarm Package: rip.RipAuthenticationMismatch Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch	Release: • N/A
Description: The alarm is raised when a peer authentication mismatch occurs. The alarm indicates the peer address.		
Remedial action: Informational - please check that RIP neighbor is sending the RIPv2 packet with the matching authentication type with this router.		

Table 39-861 RipExportLimitDropped

Alarm	Attributes	Applicable major release
Name: RipExportLimitDropped (1927) Type: configurationAlarm Package: rip.RipExportLimitDropped Raised on class: rip.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitDropped	Release: • N/A
Description: The alarm is raised when the total number of exported routes from the route table to this RIP level drops below the configured export limit		
Remedial action: Informational.		

Table 39-862 RipExportLimitReached

Alarm	Attributes	Applicable major release
Name: RipExportLimitReached (1928) Type: configurationAlarm Package: rip.RipExportLimitReached Raised on class: rip.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitReached	Release: • N/A
Description: The alarm is raised when the total number of routes for the level is equal to the configured limit for exported routes		
Remedial action: Informational - Additional routes would not be exported into RIP from the route table.		

Table 39-863 RipExportLimitWarning

Alarm	Attributes	Applicable major release
Name: RipExportLimitWarning (1929) Type: configurationAlarm Package: rip.RipExportLimitWarning Raised on class: rip.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: exportLimitWarning	Release: • N/A
Description: The alarm is raised when the number of exported routes for the RIP level equals the percentage of the export limit configured in the Export Limit Log Percent parameter.		
Remedial action: Informational - Additional routes will continue to be exported into RIP from the route table till the export limit is reached.		

Table 39-864 ripRouteMaxLimitReached

Alarm	Attributes	Applicable major release
Name: ripRouteMaxLimitReached (1090) Type: ProtocolAlarm Package: rip.ripRouteMaxLimitReached Raised on class: rip.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: maxRouteReached	Release: • N/A

Table 39-864 ripRouteMaxLimitReached (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the number of RIP routes learned by an NE exceeds the maximum specified in the RIP configuration of the NE.		
Remedial action: Informational - no corrective action required		

Table 39-865 RootDirMaxFilesReached

Alarm	Attributes	Applicable major release
Name: RootDirMaxFilesReached (3699) Type: storageAlarm Package: equipment.RootDirMaxFilesReached Raised on class: equipment.FlashMemory	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: rootDirMaxFilesReached	Release: • N/A
Description: The alarm is raised when the number of files in the root directory reaches the maximum.		
Remedial action: This alarm has been raised due the fact that the number of files in the root directory of the compact flash has gone beyond the pre-defined limit. To rectify this issue please remove unused files from the root directory.		

Table 39-866 RouterLimitExceedDueToMultiAdditions

Alarm	Attributes	Applicable major release
Name: RouterLimitExceedDueToMultiAdditions (602) Type: cpamLicensingAlarm Package: security. RouterLimitExceedDueToMultiAdditions Raised on class: security.CpamLicense	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cpamRouterLimitExceedDu-eToMultiAdditions	Release: • N/A
Description: The alarm is raised when the 5650 CPAM cannot discover one or more routers because the license capacity is reached.		
Raising condition: ('License violation due to multiple routers addition' EQUAL 'true')		
Clearing condition: ('License violation due to multiple routers addition' EQUAL 'false')		
Remedial action: Informational - The number of router (Big/Small/Multicast/Third Party) licenses purchased and available on the CPAM server is insufficient as compared to the number of big/small/multicast/third party routers under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 39-867 RouteTargetConflict

Alarm	Attributes	Applicable major release
Name: RouteTargetConflict (6447) Type: configurationAlarm Package: l3fwd.RouteTargetConflict Raised on class: l3fwd.ServiceSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: routeTargetConflictWith-OtherService	Release: • N/A

Table 39-867 RouteTargetConflict (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM detects a conflict between the configured route target on VPRN and the Reserved VPRN Table. The alarm information includes the source, i.e., import or export, and the conflict reserved VPRN RT entry distinguished name.		
Remedial action: A configuration error has occurred which should be corrected. The configured VPRN route target has a conflict with the Reserved VPRN Route Target Table. This route target has been been reserved by another service.		

Table 39-868 RouteTargetMisConfigured

Alarm	Attributes	Applicable major release
Name: RouteTargetMisConfigured (8139) Type: configurationAlarm Package: service.RouteTargetMisConfigured Raised on class: service.SvcResourceReservation	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: routeTargetMisConfigured	Release: • N/A
Description: This alarm is raised when the configured route targets associated with this Reserved Route Target entry has been misconfigured; i.e. the route target RT1 or RT2 is not configured when they are needed for associated VPRN service site creation. The affected route target's relative distinguished name is included in the alarm.		
Remedial action: A configuration error has occurred which should be corrected. This Reserved VPRN Route Target Table does not have all the configured route targets that are needed for the associated VPRN. This alarm needs to be explicitly cleared.		

Table 39-869 RowThresholdConstraintViolated

Alarm	Attributes	Applicable major release
Name: RowThresholdConstraintViolated (286) Type: configurationAlarm Package: db.RowThresholdConstraintViolated Raised on class: db.SizeConstraintPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialConstraintEnforcement	Release: • N/A
Description: The alarm is raised when the number of records in a database table exceeds the number specified in a size constraint policy.		
Raising condition: ('Cleanup partial (too many objects)' EQUAL 'true')		
Clearing condition: ('Cleanup partial (too many objects)' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 39-870 RSLHistoryUploadFailure

Alarm	Attributes	Applicable major release
Name: RSLHistoryUploadFailure (11468) Type: equipmentAlarm Package: mwa.RSLHistoryUploadFailure Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: HistoryUploadFail	Release: • N/A
Description: This alarm is raised when microwave radio RSL History upload fails.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-871 RsyncDirectoryMismatch

Alarm	Attributes	Applicable major release
Name: RsyncDirectoryMismatch (1938) Type: serverAlarm Package: server.RsyncDirectoryMismatch Raised on class: server.SamServer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: rsyncDirectoryMismatch	Release: • N/A
Description: The alarm is raised when the rsync directories on two 5620 SAM servers do not match.		
Remedial action: A configuration error has been made which must be corrected. Reconfigure the SAM servers so that the rsync directories match.		

Table 39-872 RsyncFilesToRemoteHost

Alarm	Attributes	Applicable major release
Name: RsyncFilesToRemoteHost (1939) Type: communicationsAlarm Package: server.RsyncFilesToRemoteHost Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: rsyncFilesIssue	Release: • N/A
Description: The alarm is raised when a rsync operation cannot synchronize files with the remote server.		
Remedial action: Possible causes include a HW failure on the standby SAM server or standby AUX server or loss of network connectivity between the primary and standby platforms. Establish that the platform hosting the standby SAM server or standby AUX server has not suffered a HW or network failure.		

Table 39-873 RuleRegistrationError

Alarm	Attributes	Applicable major release
Name: RuleRegistrationError (364) Type: ConfigurationAlarm Package: rules.RuleRegistrationError Raised on class: rules.RuleSet	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ruleContentsError	Release: • N/A

Table 39-873 RuleRegistrationError (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more internal 5620 SAM server rule-engine rules fails to compile. The cause is typically a rule syntax error or a system error.		
Raising condition: (('Name' EQUAL '\"N/A\"') OR ('compiled' EQUAL 'false'))		
Clearing condition: (('Name' NOT EQUAL '\"N/A\"') AND ('compiled' EQUAL 'true'))		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-874 RxDiversityMissing

Alarm	Attributes	Applicable major release
Name: RxDiversityMissing (8970) Type: equipmentAlarm Package: mwa.RxDiversityMissing Raised on class: mwa.PortTermination	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RxDiversityMissing	Release: • N/A
Description: The alarm is raised when a MPT detects missing diversity on receiver card.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-875 SapDHCPLeaseEntriesExceeded

Alarm	Attributes	Applicable major release
Name: SapDHCPLeaseEntriesExceeded (386) Type: communicationsAlarm Package: service.SapDHCPLeaseEntriesExceeded Raised on class: service.AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapDHCPLeaseEntriesExceeded	Release: • N/A
Description: The alarm is raised when the number of DHCP lease-state entries on a SAP reaches the configured maximum value. This value is defined by sapTlsDhcpLeasePopulate for a TLS VLAN service, and by vRtrIfDHCPLeasePopulate for an IES or VPRN service.		
Remedial action: The Number of DHCP lease-state entries (e.g. subscribers) on the affected interface has crossed the leasePopulate threshold defined in the DHCP Relay configuration of that interface.\nPlease review the DHCP leasePopulate configuration and adjust the number of allowed leases to meet the network requirements. Alternately, the DHCP leases can be spread out across extra interfaces.		

Table 39-876 sapDHCPLseStatePopulateErr

Alarm	Attributes	Applicable major release
Name: sapDHCPLseStatePopulateErr (3908) Type: processingErrorAlarm Package: service.sapDHCPLseStatePopulateErr Raised on class: service.AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sapDHCPLseStatePopulateError	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot update the DHCP Lease State table upon reception of a DHCP ACK message.		
Remedial action: The alarm is raised when an NE notifies the 5620 SAM that it cannot update the DHCP Lease State table upon reception of a DHCP ACK message. Verify the local DHCP server configuration or the DHCP relay configuration. Additionally, verify the length of the auto-generated subscriber identification.		

Table 39-877 sapDHCPProxyServerError

Alarm	Attributes	Applicable major release
Name: sapDHCPProxyServerError (387) Type: communicationsAlarm Package: service.sapDHCPProxyServerError Raised on class: service.AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnableProxyDHCPRequest	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to proxy a DHCP request.		
Remedial action: Please verify your DHCP relay configuration. The local proxy server will not become operational without the emulated-server address being specified. Also ensure the Proxy server state is enabled on this SAP.		

Table 39-878 SapMismatch

Alarm	Attributes	Applicable major release
Name: SapMismatch (417) Type: configurationAlarm Package: srrp.SapMismatch Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: remoteSapMismatch	Release: • N/A
Description: The alarm is raised when the SRRP SAPs on the local interface do not match the SRRP SAPs on the remote interface.		
Remedial action: Reconfigure the Service Access Interfaces for the Group Interface so that they connecting to each other for the peer SRRPs.		

Table 39-879 sapReceivedProtSrcMac

Alarm	Attributes	Applicable major release
Name: sapReceivedProtSrcMac (393) Type: accessInterfaceAlarm Package: l2fwd.sapReceivedProtSrcMac Raised on class: l2fwd.AccessInterfaceFib	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ProtectedSourceMacLearned	Release: • N/A
Description: The alarm is raised when a restricted SAP receives a re-learn request for a protected MAC address.		
Remedial action: Informational - no corrective action required.		

Table 39-880 SapStaticHost6DynamicMacConflict

Alarm	Attributes	Applicable major release
Name: SapStaticHost6DynamicMacConflict (9021) Type: configurationAlarm Package: antispoof. SapStaticHost6DynamicMacConflict Raised on class: antispoof.SapStaticIPv6Hosts	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: LearnedDynamicMacAl-readyLearned	Release: • N/A
Description: The alarm is generated when the system was unable to update the MAC address of a static IPv6 host.		
Remedial action: Informational - The NE has detected an existing FIB entry with the same MAC address, created for another IPv6 static host. Clearing the FIB entries could fix it.		

Table 39-881 SapStaticHostDynamicMacConflict

Alarm	Attributes	Applicable major release
Name: SapStaticHostDynamicMacConflict (313) Type: configurationAlarm Package: antispoof.SapStaticHostDynamicMacConflict Raised on class: antispoof.AntiSpoofingStaticHosts	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: LearnedDynamicMacAl-readyLearned	Release: • N/A
Description: The alarm is raised when an NE tries to learn a dynamic MAC address from an IP-only static host.		
Remedial action: Informational - The NE has detected an existing FIB entry with the same MAC address, created for another static host. Clearing the FIB entries could fix it.		

Table 39-882 SapTagMismatch

Alarm	Attributes	Applicable major release
Name: SapTagMismatch (418) Type: configurationAlarm Package: srrp.SapTagMismatch Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: remoteSyncTagMismatch	Release: • N/A

Table 39-882 SapTagMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the tag of a local SAP does not match the tag of a remote SAP.		
Remedial action: Reconfigure the SAPs for the peer SRRP instances so that their tags match each other.		

Table 39-883 SapVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SapVlanSubTypeConflict (290) Type: configurationAlarm Package: vlan.SapVlanSubTypeConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: topologyMisconfigured	Release: • N/A
Description: The alarm is raised when a SAP resynchronization indicates that the VLAN subtype of the SAP is different from the site subtype. The alarm information includes the ID of the associated port.		
Remedial action: Ensure that the VLAN Subtype of the SAP matches the VLAN Subtype of the Site.		

Table 39-884 SasAccountingAlarm

Alarm	Attributes	Applicable major release
Name: SasAccountingAlarm (691) Type: oamAlarm Package: sas.SasAccountingAlarm Raised on class: sas.TestSuite	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: noAccountingPolicy	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot find an SAA Accounting Policy.		
Remedial action: A configuration error has been made which must be corrected. An SAA Accounting policy is required but has not been configured - please perform the required configuration.		

Table 39-885 SasPmBinAlarmLimitReached

Alarm	Attributes	Applicable major release
Name: SasPmBinAlarmLimitReached (5413) Type: configurationAlarm Package: server.SasPmBinAlarmLimitReached Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyAlarmsRaisedByBin-Stats	Release: • N/A
Description: The alarm is raised when PM Bin Statistics has exceeded the limit of alarms for an interval.		
Remedial action: Informational - the maximum number of bin threshold alarms that can be raised in the reset interval has been reached. After the Bin alarm reset interval has passed, alarms can be raised again for the next interval until the number of alarms reaches the limit again.		

Table 39-886 SasPmBinStatThresholdExceeded

Alarm	Attributes	Applicable major release
Name: SasPmBinStatThresholdExceeded (5412) Type: misConfiguration Package: sas.SasPmBinStatThresholdExceeded Raised on class: sas.TestManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SasPmBinStatThresholdExceeded	Release: • N/A
Description: The alarm is raised if sas pm bin stats count exceeds threshold limit. This Alarm has to be cleared Manually.		
Remedial action: The alarm is raised if sas pm bin stats count exceeds Threshold Limit.This Alarm has to be cleared Manually.		

Table 39-887 SasResultCollectionThresholdExceeded

Alarm	Attributes	Applicable major release
Name: SasResultCollectionThresholdExceeded (5158) Type: misConfiguration Package: sas.SasResultCollectionThresholdExceeded Raised on class: sas.TestManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sasResultCollectionThresholdExceeded	Release: • N/A
Description: The alarm is raised if test result count exceeds maximum allowed Limit.		
Remedial action: collection Rate Greater Than expected.		

Table 39-888 SasResyncWorkerQueueOverflow

Alarm	Attributes	Applicable major release
Name: SasResyncWorkerQueueOverflow (8137) Type: misConfiguration Package: sas.SasResyncWorkerQueueOverflow Raised on class: sas.TestManager	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManySasResyncTasks	Release: • N/A
Description: The alarm is raised when incoming OAM traps can not be handled because the number of tasks that await processing on the SasResyncWorkerPool queue by the 5620 SAM surpasses the servers capacity to process them. The trap tasks mainly include incoming test results and threshold crossing events.		
Remedial action: Consider stopping some SNMP based tests or using accounting-file based tests instead. The alarm has to be cleared manually.		

Table 39-889 SasThresholdExceededAlarm

Alarm	Attributes	Applicable major release
Name: SasThresholdExceededAlarm (272) Type: oamAlarm Package: sas.SasThresholdExceededAlarm Raised on class: sas.Test	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when a rising or falling threshold is crossed by a jitter, latency, or loss value. The alarm is raised only against a scheduled test. The alarm information includes the threshold type, the threshold setting, and the current rising or falling value.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-890 SasTooManyTestsOnNodeAlarm

Alarm	Attributes	Applicable major release
Name: SasTooManyTestsOnNodeAlarm (287) Type: oamAlarm Package: sas.SasTooManyTestsOnNodeAlarm Raised on class: sas.NeAgent	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyTestsDeployedOn-Node	Release: • N/A
Description: The alarm is raised when an NE reaches 60 percent of the allowed number of created or simultaneously executed OAM tests. An attempt to create or execute an NE schedulable test on an NE fails when the number of tests reaches 95 percent of the NE capacity. The alarm information includes the following: - the NE ID - the number of deployed tests on the NE - the allowed number of deployed tests on the NE		
Remedial action: Informational - 5620 SAM is close to or at the maximum number of OAM tests it can support.		

Table 39-891 scheduledTaskCompletionStatus

Alarm	Attributes	Applicable major release
Name: scheduledTaskCompletionStatus (528) Type: taskCompletionAlarm Package: schedule.scheduledTaskCompletionStatus Raised on class: schedule.ScheduledTask	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: scheduledTaskCompleted	Release: • N/A
Description: The alarm is raised when the execution of a SAM scheduled task completes.		
Raising condition: ('Status' EQUAL 'Completed')		
Remedial action: Informational		

Table 39-892 ScriptAlarm

Alarm	Attributes	Applicable major release
Name: ScriptAlarm (5131) Type: serverAlarm Package: script.ScriptAlarm Raised on class: script.AbstractScript	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ScriptAlarm	Release: • N/A
Description: This alarm was raised from within a SAM user script when certain conditions were met, as implemented by the script author. See the alarm's 'Additional Text' for any informative details the script author may have supplied.		
Remedial action: This is an alarm generated from within a SAM user script, and therefore the remedial action will vary. See the alarm's "Additional Text" for any remedial action the script author may have supplied.		

Table 39-893 SdpBindingMisconfigured

Alarm	Attributes	Applicable major release
Name: SdpBindingMisconfigured (293) Type: SdpBindingAlarm Package: svt.SdpBindingMisconfigured Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: returnSdpBindingTypeMis-match	Release: • N/A
Description: The alarm is raised when the return SDP binding type does not match the originating SDP binding type, for example, when the return SDP binding is spoke and the originating SDP binding is mesh.		
Remedial action: A configuration error has occurred which must be corrected. The configuration on the endpoints of the SDP does not match causing the SDP to be down. Correct the configuration error and the SDP will come up.		

Table 39-894 sdpBindReceivedProtSrcMac

Alarm	Attributes	Applicable major release
Name: sdpBindReceivedProtSrcMac (3746) Type: SdpBindingAlarm Package: l2fwd.sdpBindReceivedProtSrcMac Raised on class: l2fwd.AbstractCircuitFib	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ProtectedSourceMacLearned	Release: • N/A
Description: The alarm is raised when a restricted SDP receives a re-learn request for a protected MAC address.		
Remedial action: Informational - no corrective action required.		

Table 39-895 SdpMldSnpgGrpDroppedLimitExceeded

Alarm	Attributes	Applicable major release
Name: SdpMldSnpgGrpDroppedLimitExceeded (738) Type: SdpBindingAlarm Package: vpls.SdpMldSnpgGrpDroppedLimitExceeded Raised on class: vpls.SdpBindingMldSnpgCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: igmpSnpgGrpMaxN-brGrpsReached	Release: • N/A
Description: The alarm is raised when an SDP binding drops an MLD group because the configurable maximum number of MLD groups on the SDP binding is reached.		
Remedial action: Increase the maximum number of MLD groups for the SDP binding.		

Table 39-896 sdpPbbActvPwWithNonActvCtrlPwChg

Alarm	Attributes	Applicable major release
Name: sdpPbbActvPwWithNonActvCtrlPwChg (5416) Type: processingErrorAlarm Package: svt.sdpPbbActvPwWithNonActvCtrlPwChg Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpPbbActvPwWithNonActvC-trlPwChg	Release: • N/A
Description: The alarm is raised when last pseudo-wire (PW) goes standby or down and when first PW becomes active on the Backbone Edge Bridge (BEB) where control PW is standby or down on that SDP.		
Remedial action: sdpPbbActvPwWithNonActvCtrlPwChg event with sdpPbbActvPwWithNonActvCtrlPw set to 'false' indicate clearing of sdpPbbActvPwWithNonActvCtrlPwChg with sdpPbbActvPwWithNonActvCtrlPw set to 'true'.		

Table 39-897 SecondaryBatteryFail (equipment)

Alarm	Attributes	Applicable major release
Name: SecondaryBatteryFail (3624) Type: equipmentAlarm Package: equipment.SecondaryBatteryFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: secondaryBatteryFail	Release: • N/A
Description: The alarm is raised when a secondary battery failure is detected.		
Remedial action: The battery on the CPM should be replaced or re-installed.		

Table 39-898 secondExpirationThresholdCrossed

Alarm	Attributes	Applicable major release
Name: secondExpirationThresholdCrossed (2913) Type: configurationAlarm Package: ranlicense. secondExpirationThresholdCrossed Raised on class: ranlicense.RANLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ageingLicense	Release: • N/A
Description: The alarm is raised when the specified Second Expiration Threshold for RAN licensing is crossed.		
Remedial action: Ask for a new LKDI license file with a further expiration date.		

Table 39-899 secondUsageThresholdCrossed

Alarm	Attributes	Applicable major release
Name: secondUsageThresholdCrossed (2914) Type: configurationAlarm Package: ranlicense.secondUsageThresholdCrossed Raised on class: ranlicense.RANLicense	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: insufficientPurchasedLicenses	Release: • N/A
Description: The alarm is raised when the specified Second Usage Threshold for RAN licensing is crossed.		
Remedial action: Ask for a new LKDI license file with more tokens.		

Table 39-900 SerialChannelLoopback

Alarm	Attributes	Applicable major release
Name: SerialChannelLoopback (807) Type: configurationAlarm Package: tdmequipment.SerialChannelLoopback Raised on class: tdmequipment. SerialChannelSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: serialChannelLoopback	Release: • N/A
Description: The alarm is raised when an NE reports that a serial channel has a loopback alarm condition.		
Remedial action: Informational only.		

Table 39-901 SerialControlLeadsSignalChange

Alarm	Attributes	Applicable major release
Name: SerialControlLeadsSignalChange (11191) Type: equipmentAlarm Package: tdmequipment. SerialControlLeadsSignalChange Raised on class: tdmequipment.SerialChannel	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: controlLeadStateTransition	Release: • N/A

Table 39-901 SerialControlLeadsSignalChange (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is generated when there is a change in the status of a serial control lead signal.		
Remedial action: Investigate status of attached DTE device.		

Table 39-902 ServiceMisConfigured

Alarm	Attributes	Applicable major release
Name: ServiceMisConfigured (8140) Type: configurationAlarm Package: service.ServiceMisConfigured Raised on class: service.SvcResourceReservation	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: serviceMisConfigured	Release: • N/A
Description: This alarm is raised when the VPRN service associated with a route target reservation entry has been modified, i.e., the service name is changed, or the service is deleted, or there is duplicate VPRN service with the same service and customer name detected. The associated service manager ID is attached with the alarm.		
Remedial action: A configuration error has occurred which should be corrected. The VPRN service associated with this Route Target Reservation entry has been modified, or there is duplicate VPRN service with the same service name detected.		

Table 39-903 serviceModified

Alarm	Attributes	Applicable major release
Name: serviceModified (11466) Type: communicationsAlarm Package: mpr.serviceModified Raised on class: mpr.BackhaulService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: serviceModified	Release: • N/A
Description: The alarm is raised when any modification is done post deployment of the service.		
Raising condition: (('Topology Changed' EQUAL 'true') AND ('Connect Attempted' EQUAL 'true'))		
Clearing condition: (('Topology Changed' EQUAL 'false') AND ('Connect Attempted' EQUAL 'true'))		
Remedial action: The modified service must be reconnected.		

Table 39-904 SflowCpEntrySampling

Alarm	Attributes	Applicable major release
Name: SflowCpEntrySampling (8142) Type: communicationsAlarm Package: sflow.SflowCpEntrySampling Raised on class: sflow.Receiver	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SflowCpSamplingInterrupt-edorStarted	Release: • N/A
Description: The alarm is raised when the sampling of an sFlow counter poller is interrupted or started.		

Table 39-904 SflowCpEntrySampling (continued)

Alarm	Attributes	Applicable major release
Remedial action: Counter sampling may not be available. Make sure counter poller is reachable from NE and no counter poller sequence reset happened.		

Table 39-905 SflowPacketTransmisionFailure

Alarm	Attributes	Applicable major release
Name: SflowPacketTransmisionFailure (8143) Type: communicationsAlarm Package: sflow.SflowPacketTransmisionFailure Raised on class: sflow.Receiver	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SflowPacketTxFailure	Release: • N/A
Description: The alarm is raised when an sFlow packet fails to transmit from an active sFlow receiver.		
Remedial action: Packet transmission failed.Flow data may be lost. Please check the Receiver configurations and make sure it is up and running.		

Table 39-906 SGLimitExceeded

Alarm	Attributes	Applicable major release
Name: SGLimitExceeded (456) Type: resourceAlarm Package: equipment.SGLimitExceeded Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: pimSnpgSGGroupMaxSupportedLimitExceeded	Release: • N/A
Description: The alarm is raised when the number of PIM snooping source group records on a card exceeds the maximum.		
Remedial action: Informational - The alarm is raised when the number of PIM snooping source group records on a card exceeds the maximum. To rectify this issue please increase the max number of groups for the pim snooping associated with the card. The maximum number allowed is 16,000 (S,G) entries.		

Table 39-907 ShamLinkDbDescriptAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkDbDescriptAuthFailure (663) Type: authenticationAlarm Package: ospf.ShamLinkDbDescriptAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A

Table 39-907 ShamLinkDbDescriptAuthFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE receives a dbDescript packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-908 ShamLinkDbDescriptConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkDbDescriptConfig (664) Type: configurationAlarm Package: ospf.ShamLinkDbDescriptConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a dbDescript packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-909 ShamLinkHelloAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkHelloAuthFailure (666) Type: authenticationAlarm Package: ospf.ShamLinkHelloAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-910 ShamLinkHelloConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkHelloConfig (667) Type: configurationAlarm Package: ospf.ShamLinkHelloConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-911 ShamLinkLsAckAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkLsAckAuthFailure (668) Type: authenticationAlarm Package: ospf.ShamLinkLsAckAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-912 ShamLinkLsAckConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkLsAckConfig (669) Type: configurationAlarm Package: ospf.ShamLinkLsAckConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-913 ShamLinkLsReqAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkLsReqAuthFailure (670) Type: authenticationAlarm Package: ospf.ShamLinkLsReqAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-914 ShamLinkLsReqConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkLsReqConfig (671) Type: configurationAlarm Package: ospf.ShamLinkLsReqConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-915 ShamLinkLsUpdateAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkLsUpdateAuthFailure (672) Type: authenticationAlarm Package: ospf.ShamLinkLsUpdateAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsUpdate packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-916 ShamLinkLsUpdateConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkLsUpdateConfig (673) Type: configurationAlarm Package: ospf.ShamLinkLsUpdateConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsUpdate packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-917 ShamLinkNullPacketAuthFailure

Alarm	Attributes	Applicable major release
Name: ShamLinkNullPacketAuthFailure (674) Type: authenticationAlarm Package: ospf.ShamLinkNullPacketAuthFailure Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a sham link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a null packet has been received on a sham link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-918 ShamLinkNullPacketConfig

Alarm	Attributes	Applicable major release
Name: ShamLinkNullPacketConfig (675) Type: configurationAlarm Package: ospf.ShamLinkNullPacketConfig Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a sham link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a null packet has been received on a sham link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-919 ShamLinkRxBadPacket

Alarm	Attributes	Applicable major release
Name: ShamLinkRxBadPacket (676) Type: communicationsAlarm Package: ospf.ShamLinkRxBadPacket Raised on class: ospf.ShamLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hello Applicable probable causes: • hello • dbDescript • lsReq • lsUpdate • lsAck • nullPacket	Release: • N/A
Description: The alarm is raised when an NE cannot parse an OSPF packet that it receives on a sham link.		
Remedial action: Informational - an NE cannot parse an OSPF packet that it receives on a sham link.		

Table 39-920 ShelfCPUAboveThreshold

Alarm	Attributes	Applicable major release
Name: ShelfCPUAboveThreshold (638) Type: configurationAlarm Package: equipment.ShelfCPUAboveThreshold Raised on class: equipment.HealthMonitoring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ShelfCPUUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when shelf CPU usage exceeds the threshold value.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-921 ShelfMemoryAboveThreshold

Alarm	Attributes	Applicable major release
Name: ShelfMemoryAboveThreshold (639) Type: configurationAlarm Package: equipment.ShelfMemoryAboveThreshold Raised on class: equipment.HealthMonitoring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ShelfMemoryUtilization-CrossedAboveThreshold	Release: • N/A
Description: The alarm is raised when shelf memory usage exceeds the threshold value.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-922 ShelfRxAboveThreshold

Alarm	Attributes	Applicable major release
Name: ShelfRxAboveThreshold (640) Type: configurationAlarm Package: equipment.ShelfRxAboveThreshold Raised on class: equipment.HealthMonitoring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ShelfRxUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when shelf Rx exceeds the threshold value.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-923 ShelfRxTxAboveThreshold

Alarm	Attributes	Applicable major release
Name: ShelfRxTxAboveThreshold (641) Type: configurationAlarm Package: equipment.ShelfRxTxAboveThreshold Raised on class: equipment.HealthMonitoring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ShelfRxTxUtilizationCrossed-AboveThreshold	Release: • N/A
Description: The alarm is raised when shelf Tx exceeds the threshold value.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-924 ShelfTemperatureAboveThreshold

Alarm	Attributes	Applicable major release
Name: ShelfTemperatureAboveThreshold (642) Type: configurationAlarm Package: equipment. ShelfTemperatureAboveThreshold Raised on class: equipment.HealthMonitoring	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ShelfTemperatureUtilization-CrossedAboveThreshold	Release: • N/A
Description: The alarm is raised when shelf temperature exceeds the threshold value.		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 39-925 SignalLabelMismatch

Alarm	Attributes	Applicable major release
Name: SignalLabelMismatch (3625) Type: communicationsAlarm Package: equipment.SignalLabelMismatch Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: signalLabelMismatch	Release: • N/A
Description: The alarm is raised when a signal label mismatch is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-926 SiteBgpAdVplsIdMisconfiguration

Alarm	Attributes	Applicable major release
Name: SiteBgpAdVplsIdMisconfiguration (739) Type: configurationAlarm Package: vpls.SiteBgpAdVplsIdMisconfiguration Raised on class: vpls.BgpAdSite	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bgpAdVplsIdInconsistent	Release: • N/A
Description: The alarm is raised when the configured VPLS ID on a BGP AD object differs from the VPLS ID configured for the VPLS site.		
Remedial action: The VPLS ID on a BGP AD object must match the VPLS ID configured for the VPLS site.		

Table 39-927 SiteSyncDeploymentFailure

Alarm	Attributes	Applicable major release
Name: SiteSyncDeploymentFailure (589) Type: equipmentAlarm Package: sonet.SiteSyncDeploymentFailure Raised on class: sonet.SiteSync	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: siteSyncFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM tries to deploy a value for an object when a transaction that involves the object is in progress from a different context.		
Remedial action: Another transaction is updating the object, Please try after some time.		

Table 39-928 SnmpAuthenticationFailure

Alarm	Attributes	Applicable major release
Name: SnmpAuthenticationFailure (176) Type: authenticationAlarm Package: netw.SnmpAuthenticationFailure Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authFailure	Release: • N/A

Table 39-928 SnmpAuthenticationFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an NE SNMP agent has received an SNMP message that is not properly authenticated. An NE typically does not, by default, send the notification that generates the alarm; the notification must be manually enabled through CLI.		
Remedial action: A configuration error has occurred which must be corrected. The authentication parameters for SNMP in the mediation policy is incorrect.		

Table 39-929 SnmpDaemonProblem

Alarm	Attributes	Applicable major release
Name: SnmpDaemonProblem (175) Type: communicationsAlarm Package: netw.SnmpDaemonProblem Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: snmpDaemonError	Release: • N/A
Description: The alarm is raised when one of the following occurs: - The 5620 SAM receives an unexpected response to an SNMP request, for example, when a managed NE sends the wrong object in response to an SMNP get or get-next request. - The 5620 SAM receives the TIMETRA-SYSTEM-MIB.tmnxSnmpdError trap from a managed NE.		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 39-930 SnmpDown

Alarm	Attributes	Applicable major release
Name: SnmpDown (410) Type: communicationsAlarm Package: netw.SnmpDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: snmpDown	Release: • N/A
Description: The alarm is raised when the SNMP agent is manually shut down on an NE and the NE sends a trap to indicate this.		
Remedial action: Informational		

Table 39-931 SnmpTrapDropped

Alarm	Attributes	Applicable major release
Name: SnmpTrapDropped (179) Type: communicationsAlarm Package: netw.SnmpTrapDropped Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: snmpDaemonOverloaded	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives a tmnxTrapDropped notification from an NE to indicate that the NE has dropped a trap. As a result, the 5620 SAM resynchronizes the table associated with the dropped trap.		
Remedial action: Informational.		

Table 39-932 SoftwareBootFailure

Alarm	Attributes	Applicable major release
Name: SoftwareBootFailure (107) Type: softwareAlarm Package: sw.SoftwareBootFailure Raised on class: sw.CardSoftware	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareBootProblem	Release: • N/A
Description: The alarm is raised when an NE fails to boot because of a software problem.		
Remedial action: Please contact your Nokia support representative for assistance.		

Table 39-933 SoftwareDownloading

Alarm	Attributes	Applicable major release
Name: SoftwareDownloading (109) Type: softwareAlarm Package: sw.SoftwareDownloading Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareDownloading	Release: • N/A
Description: The alarm is raised when an NE begins to download software to a IOM or CPM card.		
Remedial action: Informational		

Table 39-934 SoftwareFailureAlarm

Alarm	Attributes	Applicable major release
Name: SoftwareFailureAlarm (149) Type: softwareAlarm Package: equipment.SoftwareFailureAlarm Raised on class: equipment.ReplaceableUnit	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: loadFailed	Release: • N/A
Description: The alarm is raised when the CPM fails to load the software from the specified location. The alarm information includes the software location.		
Remedial action: The CPM card did not find the SW in the expected location. Reinstall the SW using 5620 SAM.		

Table 39-935 SoftwareInitialized

Alarm	Attributes	Applicable major release
Name: SoftwareInitialized (111) Type: softwareAlarm Package: sw.SoftwareInitialized Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareInitialized	Release: • N/A
Description: The alarm is raised when software initialization on an IOM or CPM card completes.		
Remedial action: Informational		

Table 39-936 SoftwareInitializing

Alarm	Attributes	Applicable major release
Name: SoftwareInitializing (110) Type: softwareAlarm Package: sw.SoftwareInitializing Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: softwareInitializing	Release: • N/A
Description: The alarm is raised when software initialization on an IOM or CPM card begins.		
Remedial action: Informational		

Table 39-937 SoftwareUpgradeFailed

Alarm	Attributes	Applicable major release
Name: SoftwareUpgradeFailed (106) Type: configurationAlarm Package: sw.SoftwareUpgradeFailed Raised on class: sw.SoftwareUpgradeManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileAccessError	Release: • N/A
Description: The alarm is raised when an NE software upgrade using the 5620 SAM fails.		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 39-938 SonetSDHLoopback

Alarm	Attributes	Applicable major release
Name: SonetSDHLoopback (407) Type: configurationAlarm Package: sonetequipment.SonetSDHLoopback Raised on class: sonetequipment.SonetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sonetSDHLoopback	Release: • N/A
Description: The alarm is raised when a loopback test is provisioned on a SONET/SDH port.		
Remedial action: Remove the loopback test from the SONET/SDH port.		

Table 39-939 sourceSapChange

Alarm	Attributes	Applicable major release
Name: sourceSapChange (4813) Type: ConfigurationAlarm Package: mirror.sourceSapChange Raised on class: mirror.SourceInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tMirrorSourceSapChange	Release: • N/A
Description: The alarm is raised when a SAP that is associated with this mirror source is modified or deleted.		

Table 39-939 sourceSapChange (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 39-940 SpbNbrMultAdjExists

Alarm	Attributes	Applicable major release
Name: SpbNbrMultAdjExists (4394) Type: configurationAlarm Package: spb.SpbNbrMultAdjExists Raised on class: spb.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: multiAdj	Release: • N/A
Description: The alarm is sent when IS-IS SPB instance detects a neighbor to which it already has a direct adjacency on another interface.		
Remedial action: Check number of links to neighbor to make sure there is only one SPB link.		

Table 39-941 SpbRejectedAdjacency

Alarm	Attributes	Applicable major release
Name: SpbRejectedAdjacency (4395) Type: adjacencyAlarm Package: spb.SpbRejectedAdjacency Raised on class: spb.AbstractInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM receives a vRtrIsisRejectedAdjacency trap, which indicates that an adjacency cannot be established in response to a Hello PDU from an IS because of a lack of resources.		
Remedial action: Informational, might have exceeded the maximum number of adjacencies allowed.		

Table 39-942 SRGMismatchAlarm

Alarm	Attributes	Applicable major release
Name: SRGMismatchAlarm (8423) Type: integrityViolation Package: gmpls.SRGMismatchAlarm Raised on class: gmpls.TeLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: srgMismatch	Release: • N/A
Description: The alarm is raised when the SRGs configured on the endpoints of the TE Link do not match.		
Remedial action: This alarm indicates that the SRGs configured on the endpoints of the discovered TE Link do not match. Please make sure the SRGs match.		

Table 39-943 SSHLoginMaxAttempts

Alarm	Attributes	Applicable major release
Name: SSHLoginMaxAttempts (3702) Type: communicationsAlarm Package: netw.SSHLoginMaxAttempts Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: sshLoginMaxAttempts	Release: • N/A
Description: The alarm is raised when the number of CLI login failures due to incorrect user name or password using SSH session exceeds the configured value.		
Remedial action: The wrong password was entered by the user during SSH. Please try to log in again later.		

Table 39-944 SSHServerPreserveKeyFailure

Alarm	Attributes	Applicable major release
Name: SSHServerPreserveKeyFailure (406) Type: softwareAlarm Package: equipment.SSHServerPreserveKeyFailure Raised on class: equipment.FlashMemory	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: preserveKeyFailure	Release: • N/A
Description: The alarm is raised when the CPM fails to save the SSH server host key on the persistent drive.		
Remedial action: Information - if the alarm persists please contact your Nokia support representative for assistance.		

Table 39-945 SSLKeystoreCertificateExpired

Alarm	Attributes	Applicable major release
Name: SSLKeystoreCertificateExpired (5138) Type: serverAlarm Package: server.SSLKeystoreCertificateExpired Raised on class: server.SamServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSLKeystoreCertificateHasExpired	Release: • N/A
Description: The alarm is raised when the SSL Keystore certificate for 5620 SAM has expired.		
Remedial action: Please reconfigure 5620 SAM with an unexpired SSL Keystore Certificate. Please refer to the 5620 SAM Installation and Upgrade guide.		

Table 39-946 SSLKeystoreCertificateExpiring

Alarm	Attributes	Applicable major release
Name: SSLKeystoreCertificateExpiring (5139) Type: serverAlarm Package: server.SSLKeystoreCertificateExpiring Raised on class: server.SamServer	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SSLKeystoreCertificateAboutToExpire	Release: • N/A

Table 39-946 SSLKeystoreCertificateExpiring (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the 5620 SAM SSL Keystore certificate is expiring soon.		
Remedial action: Please reconfigure 5620 SAM with a newer SSL Keystore Certificate. Please refer to the 5620 SAM Installation and Upgrade guide.		

Table 39-947 StandbyArchiveLogDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: StandbyArchiveLogDiskSpaceBelowThreshold (2936) Type: databaseAlarm Package: db.StandbyArchiveLogDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the standby database archived log disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: Adequate disk space should be allocated on the database servers for archive log files. Performing a manual database backup is required to reduce the size of this directory. If the alarm persists then the frequency of database backups must be increased.		

Table 39-948 StandbyCPMManagementConnectionDown

Alarm	Attributes	Applicable major release
Name: StandbyCPMManagementConnectionDown (140) Type: communicationsAlarm Package: netw.StandbyCPMManagementConnectionDown Raised on class: netw.NodeDiscoveryControl	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: managementConnectionDown	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot reach a managed NE using the ping function.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM		

Table 39-949 StandbyDataFileDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: StandbyDataFileDiskSpaceBelowThreshold (539) Type: databaseAlarm Package: db.StandbyDataFileDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the standby data file disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-950 StandbyInstallDirectoryDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: StandbyInstallDirectory-DiskSpaceBelowThreshold (615) Type: databaseAlarm Package: db.StandbyInstallDirectoryDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the standby database installation disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The Oracle Proxy purges the log based on database file policy configuration. Reducing the number of archives to keep and/or size of the log files or increasing the available disk space will resolve the problem. If alarm persists please contact your Nokia support representative for assistance.		

Table 39-951 StandbyOracleHomeDiskSpaceBelowThreshold

Alarm	Attributes	Applicable major release
Name: StandbyOracleHomeDiskSpaceBe-lowThreshold (540) Type: databaseAlarm Package: db.StandbyOracleHomeDiskSpaceBelowThreshold Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when the standby database Oracle disk space threshold specified in the nms-server.xml file is reached.		
Remedial action: The Oracle Proxy purges the log based on database file policy configuration. Reducing the number of archives to keep and/or size of the log files or increasing the available disk space will resolve the problem. If alarm persists please contact your Nokia support representative for assistance.		

Table 39-952 StandbyServerStatus

Alarm	Attributes	Applicable major release
Name: StandbyServerStatus (208) Type: communicationsAlarm Package: netw.StandbyServerStatus Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when the primary 5620 SAM main server cannot communicate with the 5620 SAM standby main server. The alarm clears when communication between the servers is restored.		
Remedial action: Informational		

Table 39-953 StatisticsCollectionThresholdExceeded

Alarm	Attributes	Applicable major release
Name: StatisticsCollectionThresholdExceeded (524) Type: communicationsAlarm Package: netw.StatisticsCollectionThresholdExceeded Raised on class: netw.NmsSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: collectionRateGreater-ThanConfigured	Release: • N/A
Description: The alarm is raised when the accounting statistics collection rate exceeds the retention specifications.		
Remedial action: The rate at which accounting statistics are being collected must be reduced or the amount of disk space allocated to accounting statistics storage must be increased. Note that the latter may require adding additional disk space to the system to resolve the problem.		

Table 39-954 StatsPollerProblem

Alarm	Attributes	Applicable major release
Name: StatsPollerProblem (5404) Type: communicationsAlarm Package: netw.StatsPollerProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to poll a network stats object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 39-955 STMSystemMultiAuxAvailable

Alarm	Attributes	Applicable major release
Name: STMSystemMultiAuxAvailable (527) Type: misConfiguration Package: sas.STMSystemMultiAuxAvailable Raised on class: sas.TestManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: multiAuxiliaryServersAvailable	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects multiple available auxiliary servers for test execution.		
Remedial action: Reserved for future use		

Table 39-956 STMSystemNotAvailable

Alarm	Attributes	Applicable major release
Name: STMSystemNotAvailable (526) Type: communicationsAlarm Package: sas.STMSystemNotAvailable Raised on class: sas.TestManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: noAuxiliaryServersAvailable	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects no available auxiliary servers for test execution.		
Remedial action: Reserved for future use		

Table 39-957 STMTestIdRangeMistmatch

Alarm	Attributes	Applicable major release
Name: STMTestIdRangeMistmatch (792) Type: oamAlarm Package: sas.STMTestIdRangeMistmatch Raised on class: sas.TestManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: testIdRangeMismatch	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects an STM test ID range mismatch between the primary and standby main servers.		
Remedial action: The configuration on the primary and standby servers must be aligned to resolve this problem. Please contact your Nokia support representative for assistance.		

Table 39-958 STMTestsOutsideRange

Alarm	Attributes	Applicable major release
Name: STMTestsOutsideRange (793) Type: oamAlarm Package: sas.STMTestsOutsideRange Raised on class: sas.TestManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: testsOutsideRange	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects one or more STM Tests that have IDs outside the specified range.		

Table 39-958 STMTestsOutsideRange (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The testId in a STM test definition must be within the testId range specified within the nms-server.xml file		

Table 39-959 STMTrailDown

Alarm	Attributes	Applicable major release
Name: STMTrailDown (9001) Type: communicationsAlarm Package: optical.STMTrailDown Raised on class: optical.STMTrail	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the STM trail are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-960 SubIpoeInvalidCidRidChange (service)

Alarm	Attributes	Applicable major release
Name: SubIpoeInvalidCidRidChange (8412) Type: processingErrorAlarm Package: service.SubIpoeInvalidCidRidChange Raised on class: service.GroupInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeInvalidCidRidChange	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session due to an invalid Circuit ID or Remote ID change.		
Remedial action: The IPoE session Circuit ID or Remote ID change is invalid. Review the alarm's additional text for further details.		

Table 39-961 SubIpoeInvalidCidRidChange (vpls)

Alarm	Attributes	Applicable major release
Name: SubIpoeInvalidCidRidChange (8412) Type: processingErrorAlarm Package: vpls.SubIpoeInvalidCidRidChange Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeInvalidCidRidChange	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session due to an invalid Circuit ID or Remote ID change.		
Remedial action: The IPoE session Circuit ID or Remote ID change is invalid. Review the alarm's additional text for further details.		

Table 39-962 SubIpoeInvalidSessionKey (service)

Alarm	Attributes	Applicable major release
Name: SubIpoeInvalidSessionKey (8413) Type: processingErrorAlarm Package: service.SubIpoeInvalidSessionKey Raised on class: service.GroupInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeInvalidSessionKey	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session due to an invalid session key.		
Remedial action: There is a mismatch between the session key sent by the Access Node and the session key configured in the IPoE session policy. Check the configuration and ensure that it matches. Review the alarm's additional text for further details.		

Table 39-963 SubIpoeInvalidSessionKey (vpls)

Alarm	Attributes	Applicable major release
Name: SubIpoeInvalidSessionKey (8413) Type: processingErrorAlarm Package: vpls.SubIpoeInvalidSessionKey Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeInvalidSessionKey	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session due to an invalid session key.		
Remedial action: There is a mismatch between the session key sent by the Access Node and the session key configured in the IPoE session policy. Check the configuration and ensure that it matches. Review the alarm's additional text for further details.		

Table 39-964 SubIPoEMigrationHostDelete (vpls)

Alarm	Attributes	Applicable major release
Name: SubIPoEMigrationHostDelete (9596) Type: processingErrorAlarm Package: vpls.SubIPoEMigrationHostDelete Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIPoEMigrationHostDelete	Release: • N/A
Description: The alarm is raised when system deletes a host for IPoE session migration.		
Remedial action: No action required. The system is performing an IPoE session migration.		

Table 39-965 SubIPoEMigrationHostDelete (service)

Alarm	Attributes	Applicable major release
Name: SubIPoEMigrationHostDelete (9596) Type: processingErrorAlarm Package: service.SubIPoEMigrationHostDelete Raised on class: service.GroupInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIPoEMigrationHostDelete	Release: • N/A
Description: The alarm is raised when system deletes a host for IPoE session migration.		

Table 39-965 SubIPoEMigrationHostDelete (service) (continued)

Alarm	Attributes	Applicable major release
Remedial action: No action required. The system is performing an IPoE session migration.		

Table 39-966 SubIpoePersistenceRecovery (vpls)

Alarm	Attributes	Applicable major release
Name: SubIpoePersistenceRecovery (8414) Type: processingErrorAlarm Package: vpls.SubIpoePersistenceRecovery Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoePersistenceRecovery	Release: • N/A
Description: The alarm is raised when the NE fails to initialize an IPoE session because it is busy re-initiating objects from persistence files.		
Remedial action: No action required. IPoE Session creation will resume once the NE has finished recovering all persisted objects.		

Table 39-967 SubIpoePersistenceRecovery (service)

Alarm	Attributes	Applicable major release
Name: SubIpoePersistenceRecovery (8414) Type: processingErrorAlarm Package: service.SubIpoePersistenceRecovery Raised on class: service.GroupInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoePersistenceRecovery	Release: • N/A
Description: The alarm is raised when the NE fails to initialize an IPoE session because it is busy re-initiating objects from persistence files.		
Remedial action: No action required. IPoE Session creation will resume once the NE has finished recovering all persisted objects.		

Table 39-968 SubIpoeSessionLimitReached (vpls)

Alarm	Attributes	Applicable major release
Name: SubIpoeSessionLimitReached (8415) Type: processingErrorAlarm Package: vpls.SubIpoeSessionLimitReached Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeSessionLimitReached	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session because the IPoE session limit is reached.		
Remedial action: The total number of IPoE sessions exceed the session limit. Additional sessions cannot be created. Increase the Session Limit/SAP Session Limit in the IES/VPRN Group Interface.		

Table 39-969 SubIpoeSessionLimitReached (service)

Alarm	Attributes	Applicable major release
Name: SubIpoeSessionLimitReached (8415) Type: processingErrorAlarm Package: service.SubIpoeSessionLimitReached Raised on class: service.GroupInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubIpoeSessionLimitReached	Release: • N/A
Description: The alarm is raised when this system fails to create an IPoE session because the IPoE session limit is reached.		
Remedial action: The total number of IPoE sessions exceed the session limit. Additional sessions cannot be created. Increase the Session Limit/SAP Session Limit in the IES/VPRN Group Interface.		

Table 39-970 SubMngdHostCreationFail

Alarm	Attributes	Applicable major release
Name: SubMngdHostCreationFail (10270) Type: processingErrorAlarm Package: vpls.SubMngdHostCreationFail Raised on class: vpls.L2AccessInterface	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subMngdHostCreationFail	Release: • N/A
Description: The alarm indicates an attempt to create a managed host has failed. [CAUSE] A failure occurs while trying to create a managed host. [EFFECT] The context for the managed host is not created. The system cannot provide network connectivity to the host. [RECOVERY] The recovery action depends on the root cause of the failure. The root cause may be a misconfiguration in the client device, the access network, in this system, or in the AAA server configuration.		
Remedial action: The recovery action depends on the root cause of the failure. The root cause may be a misconfiguration in the client device, the access network, in this system, or in the AAA server configuration.		

Table 39-971 SubMngdHostOverride

Alarm	Attributes	Applicable major release
Name: SubMngdHostOverride (10269) Type: processingErrorAlarm Package: service.SubMngdHostOverride Raised on class: service.ServiceAccessPoint	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubMngdHostOverride	Release: • N/A
Description: [CAUSE] The alarm indicates a new managed host replaces an existing host with the same IP address. [EFFECT] The existing host is removed from the system. [RECOVERY] None.		
Remedial action: The alarm is raised when a new managed host replaces an existing host with the same IP address. No action is required.		

Table 39-972 SubnetBindingFailed

Alarm	Attributes	Applicable major release
Name: SubnetBindingFailed (4988) Type: processingErrorAlarm Package: dhcp.SubnetBindingFailed Raised on class: dhcp.AddressPool	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tmnxDhcpSvrSubnetBinding-Failed	Release: • N/A
Description: This alarm is raised when a DHCP server instance cannot offer an IP address to a host, because a subnet binding with its access node (service) is required but not available anymore in the pool.		
Remedial action: The configuration of the Local DHCP Server IP Address Pool and/or the access node (service) must be changed in order to make more subnets available.		

Table 39-973 SubnetFailCtrlError

Alarm	Attributes	Applicable major release
Name: SubnetFailCtrlError (5156) Type: configurationAlarm Package: dhcp.SubnetFailCtrlError Raised on class: dhcp.Subnet	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: leaseWithInconsistent-FailoverConfiguration	Release: • N/A
Description: The alarm is raised each time a lease is created in a subnet with an inconsistent failover configuration		
Remedial action: A subnet lease has an inconsistent failover configuration, where the failover control type is not identical for all subnet ranges while the pool subnet binding key is not equal to 'none'. Please restore consistency of the failover control configuration for all subnet ranges in this subnet.		

Table 39-974 SubnetMismatch

Alarm	Attributes	Applicable major release
Name: SubnetMismatch (415) Type: configurationAlarm Package: srrp.SubnetMismatch Raised on class: srrp.Instance	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ipAddressListMismatch	Release: • N/A
Description: The alarm is raised when the IP address list received from the master does not match the local IP address list.		
Remedial action: Check the IP address of the Subscriber interface and make sure the address for the peer SRRP instances are in the same subnet.		

Table 39-975 SubRackBatteryFail

Alarm	Attributes	Applicable major release
Name: SubRackBatteryFail (5426) Type: equipmentAlarm Package: mpr.SubRackBatteryFail Raised on class: mpr.SubRack	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: batteryFail	Release: • N/A
Description: The alarm is raised when the battery fails or is missing on SubRack.		
Remedial action: The battery on the subrack should be replaced or re-installed.		

Table 39-976 SubRackSecondaryBatteryFail

Alarm	Attributes	Applicable major release
Name: SubRackSecondaryBatteryFail (5427) Type: equipmentAlarm Package: mpr.SubRackSecondaryBatteryFail Raised on class: mpr.SubRack	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: secondaryBatteryFail	Release: • N/A
Description: The alarm is raised when a secondary battery failure is detected on SubRack.		
Remedial action: The battery on the subrack should be replaced or re-installed.		

Table 39-977 SubscrAuthPolicyMisconfigured (vpls)

Alarm	Attributes	Applicable major release
Name: SubscrAuthPolicyMisconfigured (271) Type: ConfigurationAlarm Package: vpls.SubscrAuthPolicyMisconfigured Raised on class: vpls.L2AccessItfDhcpRelayCfg	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SubscrAuthPolicyNotFound	Release: • N/A
Description: The alarm is raised when a subscriber authentication policy for DHCP relay is misconfigured.		
Remedial action: Check the local and global configuration for the subscriber authentication policy for DHCP relay.		

Table 39-978 SubscrAuthPolicyMisconfigured (rtr)

Alarm	Attributes	Applicable major release
Name: SubscrAuthPolicyMisconfigured (271) Type: ConfigurationAlarm Package: rtr.SubscrAuthPolicyMisconfigured Raised on class: rtr.VirtualInterfaceConfiguration	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SubscrAuthPolicyNotFound	Release: • N/A
Description: The alarm is raised when a subscriber authentication policy for DHCP relay is misconfigured.		
Remedial action: This alarm is raised on L2 and L3 access interfaces when the authentication policy specified for DHCP Relay does not exist. Please make sure to select an authentication policy that exists or to configure a new authentication policy with that name.		

Table 39-979 SubscriberMisConfigured

Alarm	Attributes	Applicable major release
Name: SubscriberMisConfigured (8141) Type: configurationAlarm Package: service.SubscriberMisConfigured Raised on class: service.SvcResourceReservation	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: subscriberMisConfigured	Release: • N/A
Description: This alarm is raised when the customer associated with a route target reservation entry has been modified, i.e., the customer name can be changed, or the customer is deleted.		
Remedial action: A configuration error has occurred which should be corrected. This customer associated with the Reserved VPRN Route Target Table has been modified.		

Table 39-980 SubSlaacOverride

Alarm	Attributes	Applicable major release
Name: SubSlaacOverride (5414) Type: processingErrorAlarm Package: service.SubSlaacOverride Raised on class: service.ServiceAccessPoint	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: subSlaacAddressOverlap	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that an IPv6 client requests a DHCPv6 non-temporary address (IA_NA) which overrides an existing SLAAC prefix that is assigned to a host. This configuration causes the SLAAC host to be removed from the system.		
Remedial action: Provide a non-overlapping IPv6 Address for the SLAAC host.		

Table 39-981 SubSlaacSetupFailure

Alarm	Attributes	Applicable major release
Name: SubSlaacSetupFailure (3906) Type: processingErrorAlarm Package: service.SubSlaacSetupFailure Raised on class: service.ServiceAccessPoint	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SubSlaacSetupFailure	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot create or update a SLAAC host in the tmnxSubSlaacTable.		
Remedial action: The alarm is raised when an NE notifies SAM that it cannot create or update a SLAAC host in the tmnxSubSlaacTable. Verify the service configuration.		

Table 39-982 SubVirtualSubnetHostsDeleted

Alarm	Attributes	Applicable major release
Name: SubVirtualSubnetHostsDeleted (5411) Type: configurationAlarm Package: ressubscr.SubVirtualSubnetHostsDeleted Raised on class: ressubscr.ResidentialSubscriberInstance	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: subVirtualSubnetHostsDeleted	Release: • N/A
Description: This alarm is raised when the NE deletes all existing hosts for a subscriber associated with a virtual subnet because a new default router and/or subnet were assigned. This is the consequence of a configuration change on the server that assigns the subnet.		
Remedial action: The hosts must transmit DHCP requests if they require a connection.		

Table 39-983 svcArpHostPopulateErr

Alarm	Attributes	Applicable major release
Name: svcArpHostPopulateErr (3909) Type: processingErrorAlarm Package: service.svcArpHostPopulateErr Raised on class: service.AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: svcArpHostPopulateError	Release: • N/A
Description: The alarm is raised when an NE notifies the 5620 SAM that it cannot update the ARP Host table upon reception of an ARP message.		
Remedial action: The alarm is raised when an NE notifies the 5620 SAM that it cannot update the ARP Host table upon reception of an ARP message. Verify the service configuration. Additionally, verify the length of the auto-generated subscriber identification.		

Table 39-984 svcFdbMimDestTableFull

Alarm	Attributes	Applicable major release
Name: svcFdbMimDestTableFull (588) Type: resourceAlarm Package: netw.svcFdbMimDestTableFull Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • N/A
Description: The alarm is raised when the number of backbone MAC address indices on an NE reaches the maximum allowed value. The alarm clears when the number of backbone MAC address indices on the NE falls below 95 percent of the maximum allowed value.		
Remedial action: Informational		

Table 39-985 SvcNameUpgradeScriptFailed

Alarm	Attributes	Applicable major release
Name: SvcNameUpgradeScriptFailed (1082) Type: scriptAlarm Package: netw.SvcNameUpgradeScriptFailed Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cliConnectionFailed Applicable probable causes: • cliConnectionFailed • cliLoginFailed • executionFailed	Release: • N/A
Description: The alarm is raised when a generated NE-upgrade CLI script fails. Typical causes include the following: - invalid CLI login information in the mediation policy - an unreachable NE Manual script execution from the NE properties form may provide more information about the failure.		
Remedial action: The alarm is raised in the following scenarios: the NE is unreachable; security credential issues. The remedial actions for the scenarios above are respectively as follows: NE unreachable - investigate and resolve the underlying transport network issue;		

Table 39-986 SWIncompatibility

Alarm	Attributes	Applicable major release
Name: SWIncompatibility (471) Type: configurationAlarm Package: equipment.SWIncompatibility Raised on class: equipment.StackConfiguration	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: elementNotCompatibleWith-ExistingStack	Release: • N/A
Description: The alarm is raised when a slot is not compatible with the current stack. The slot subsequently enters pass-through mode.		
Remedial action: Login to switch console, and install same software load on primary and secondary slot and synchronize them and reload switch.		

Table 39-987 SwitchOverDatabase

Alarm	Attributes	Applicable major release
Name: SwitchOverDatabase (203) Type: configurationAlarm Package: db.SwitchOverDatabase Raised on class: db.DatabaseManager	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: switchOverDatabase	Release: • N/A
Description: The alarm is raised when a database switchover occurs.		
Remedial action: Informational - no corrective action required.		

Table 39-988 SwitchOverDatabaseFailed

Alarm	Attributes	Applicable major release
Name: SwitchOverDatabaseFailed (204) Type: configurationAlarm Package: db.SwitchOverDatabaseFailed Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: switchOverDatabaseFailed	Release: • N/A
Description: The alarm is raised when a database switchover fails.		
Remedial action: The additional text field of the alarm will provide more details as will the EmsServer.log. Possible causes include a HW failure on the platform hosting the database function, loss of network connectivity between the primary and standby database platforms. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-989 SychronizationLossOfSignal

Alarm	Attributes	Applicable major release
Name: SychronizationLossOfSignal (799) Type: communicationsAlarm Package: equipment.SychronizationLossOfSignal Raised on class: equipment.Shelf	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lossOfSignal	Release: • N/A
Description: The alarm is raised when an SLOS signal is detected on a PDH tributary.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-990 SyncCertFailed

Alarm	Attributes	Applicable major release
Name: SyncCertFailed (3912) Type: equipmentAlarm Package: sitesec.SyncCertFailed Raised on class: sitesec.SiteSystemSecurityPublicKey	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SyncCertFailed	Release: • N/A
Description: The alarm is raised when the synchronization of certificate files between the primary and secondary CPMs is stopped due to errors.		
Remedial action: The synchronization of certificate files between the primary and secondary CPMs is stopped due to errors. Depending on the reason specified, corrective action should be taken		

Table 39-991 synchroFailureAlarm

Alarm	Attributes	Applicable major release
Name: synchroFailureAlarm (534) Type: softwareAlarm Package: sw.synchroFailureAlarm Raised on class: sw.SoftwareControlModule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: synchroFailureAlarm	Release: • N/A
Description: The alarm is raised when the flash card synchronization on an NE fails.		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 39-992 SystemCorruption

Alarm	Attributes	Applicable major release
Name: SystemCorruption (9582) Type: equipmentAlarm Package: netw.SystemCorruption Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: SystemCorruption	Release: • N/A
Description: The alarm is raised when a client-specific persistence event occurs (e.g. the start and completion of a recover action after system startup).		
Remedial action: Please perform a file repair.		

Table 39-993 SystemMemoryConsumption

Alarm	Attributes	Applicable major release
Name: SystemMemoryConsumption (225) Type: communicationsAlarm Package: netw.SystemMemoryConsumption Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyTrapsBuffered	Release: • N/A
Description: The alarm is raised when the global number of SNMP traps that await processing by the 5620 SAM surpasses the system red threshold for trap memory management specified in the base configuration of the 5620 SAM server. Caution: Nokia strongly recommends against modifying NE trap management threshold values; modifying these values can seriously degrade 5620 SAM performance. The alarm clears when the number of traps that await processing falls below the system red threshold. The 5620 SAM resynchronizes the NEs, if required.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

Table 39-994 SystemModeChange

Alarm	Attributes	Applicable major release
Name: SystemModeChange (1923) Type: equipmentAlarm Package: optical.SystemModeChange Raised on class: optical.OpticalNeProperties	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: systemModeChange	Release: • N/A
Description: The alarm is raised when an NE undergoes a system mode change, for example, from SONET to SDH mode. The alarm information includes the Site ID, old system mode value and new system mode value.		
Remedial action: Informational.The alarm is raised when an NE undergoes a system mode change, for ex. from SONET to SDH mode.		

Table 39-995 SystemNameChange

Alarm	Attributes	Applicable major release
Name: SystemNameChange (228) Type: equipmentAlarm Package: netw.SystemNameChange Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemNameChange	Release: • N/A
Description: The alarm is raised when an NE undergoes a system name change. The alarm information includes the old system name and the new system name.		
Remedial action: Informational - this alarm indicates that the name of the NE has been changed via CLI directly on the NE. The new name will not appear in the SAM GUI. Unmanage and re-manage this node for new name to take effect. Please contact your Nokia support representative for assistance.		

Table 39-996 TableSpaceAboveThreshold

Alarm	Attributes	Applicable major release
Name: TableSpaceAboveThreshold (454) Type: databaseAlarm Package: db.TableSpaceAboveThreshold Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: HighStatisticsCollectionRate	Release: • N/A
Description: The alarm is raised when the database table space becomes too full, which may indicate that the performance statistics collection rate or the statistics retention time is too high.		
Remedial action: Purging the performance statistics log records, reducing the performance statistics retention time or reducing the frequency of collection should resolve this issue. If this is not possible then it may be necessary to add additional disk capacity to the platform. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-997 TCAAlarmLimitReached

Alarm	Attributes	Applicable major release
Name: TCAAlarmLimitReached (3687) Type: configurationAlarm Package: server.TCAAlarmLimitReached Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyAlarmsRaisedByTCA	Release: • N/A
Description: The alarm is raised when a TCA execute server reaches the limit of alarms for an interval.		
Remedial action: Informational - the maximum number of threshold crossing alarms that can be raised in the reset interval has been reached. After the TCA alarm reset interval has passed, alarms can be raised again for the next interval until the number of alarms reaches the limit again.		

Table 39-998 TCEAssignmentProblem

Alarm	Attributes	Applicable major release
Name: TCEAssignmentProblem (5140) Type: processingErrorAlarm Package: server.TCEAssignmentProblem Raised on class: server.TCE	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: configurationOrCustomization-Error	Release: • N/A
Description: This alarm is raised when the NE state does not allow SAM to assign the NE to the TCE during the load balancing or the manual operator assignment.\nSAM automatically clears the TCE alarm on succeeded assignment.		
Remedial action: Ensure the NE is managed, reachable and that no configuration operation is in progress on that NE and relaunch the operation.		

Table 39-999 TChipMemoryError

Alarm	Attributes	Applicable major release
Name: TChipMemoryError (5183) Type: hardwareAnomaly Package: equipment.TChipMemoryError Raised on class: equipment.BaseCard	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tchipMemoryParityError	Release: • N/A
Description: This Alarm is raised when a T-chip experiences an occurrence of an internal memory parity error.		
Remedial action: A fault has been detected in the hardware. If the problem persists please contact your Nokia support representative for assistance.		

Table 39-1000 TCMonitorMismatchAlarm

Alarm	Attributes	Applicable major release
Name: TCMonitorMismatchAlarm (8424) Type: integrityViolation Package: gmpls.TCMonitorMismatchAlarm Raised on class: gmpls.DbLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tcmMismatch	Release: • N/A
Description: The alarm is raised when the TCM configured on the endpoints of the DB Link do not match.		
Remedial action: This alarm indicates that the TCM configured on the endpoints of the discovered DB Link do not match. Please make sure the TCM is the same on the databearers at each end.		

Table 39-1001 TeLinkPropertyMismatch

Alarm	Attributes	Applicable major release
Name: TeLinkPropertyMismatch (8392) Type: operationalViolation Package: lmp.TeLinkPropertyMismatch Raised on class: lmp.TeLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: propertyMismatch	Release: • N/A
Description: The alarm is raised when a Traffic-Engineering Link property mismatch is detected on the node. This notification is only generated the first time a mismatch is detected.		
Remedial action: A network configuration issue has been detected. Ensure the Traffic-Engineering Link configuration between the local node and the peer node is consistent.		

Table 39-1002 TemplateInconsistency

Alarm	Attributes	Applicable major release
Name: TemplateInconsistency (189) Type: ConfigurationAlarm Package: policy.TemplateInconsistency Raised on class: policy.PolicyDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: templatePolicyMismatch	Release: • N/A
Description: The alarm is raised when there is a parameter type or value mismatch between a global policy and a local policy.		
Remedial action: Informational - this alarm indicates that during the a policy comparison audit a mismatch was detected between local policy deployed on a NE vs the global policy which was used to perform the original configuration on NE. Re-distributing the global policy to the outlined NE and/or re-configuring the distribution mode of the local policy to be Sync With Global.		

Table 39-1003 TemporaryCommunicationFailure

Alarm	Attributes	Applicable major release
Name: TemporaryCommunicationFailure (800) Type: equipmentAlarm Package: equipment.TemporaryCommunicationFailure Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: temporaryCommunication-Problem	Release: • N/A
Description: The alarm is raised when a temporary communication failure is detected.		
Remedial action: 5620 SAM has temporarily lost contact with an NE. This may have been caused by the NE restarting, the NE being taken off-line via operator intervention or by a loss of connectivity to the NE. If the NE restarted then there will be an alarm indicating th		

Table 39-1004 TestFailedAlarm (bgp)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: bgp.TestFailedAlarm Raised on class: bgp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1005 TestFailedAlarm (mirror)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: mirror.TestFailedAlarm Raised on class: mirror.Mirror	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1006 TestFailedAlarm (mpls)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: mpls.TestFailedAlarm Raised on class: mpls.Lsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1006 TestFailedAlarm (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1007 TestFailedAlarm (svt)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: svt.TestFailedAlarm Raised on class: svt.Tunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1008 TestFailedAlarm (ldp)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: ldp.TestFailedAlarm Raised on class: ldp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1009 TestFailedAlarm (pim)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: pim.TestFailedAlarm Raised on class: pim.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1010 TestFailedAlarm (rtr)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: rtr.TestFailedAlarm Raised on class: rtr.VirtualRouter	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1011 TestFailedAlarm (vprn)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: vprn.TestFailedAlarm Raised on class: vprn.Vprn	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1012 TestFailedAlarm (netw)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: netw.TestFailedAlarm Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when TestFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1013 TestFailedAlarm (service)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: service.TestFailedAlarm Raised on class: service.SpokeConnector	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1013 TestFailedAlarm (service) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when TestFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1014 TestFailedAlarm (lte)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: lte.TestFailedAlarm Raised on class: lte.EPSPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when TestFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1015 TestFailedAlarm (ethernetoam)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: ethernetoam.TestFailedAlarm Raised on class: ethernetoam.MaintAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1016 TestFailedAlarm (mplstp)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: mplstp.TestFailedAlarm Raised on class: mplstp.TPLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1017 TestFailedAlarm (lteservice)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: lteservice.TestFailedAlarm Raised on class: lteservice.MobileService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1018 TestFailedAlarm (monpath)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: monpath.TestFailedAlarm Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1019 TestFailedAlarm (vll)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: vll.TestFailedAlarm Raised on class: vll.Vll	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1020 TestFailedAlarm (atm)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: atm.TestFailedAlarm Raised on class: atm.PvcConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1020 TestFailedAlarm (atm) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1021 TestFailedAlarm (vpls)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm (3708) Type: oamAlarm Package: vpls.TestFailedAlarm Raised on class: vpls.AbstractVpls	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1022 TestFailedAlarm2 (ethernetoam)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: ethernetoam.TestFailedAlarm2 Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1023 TestFailedAlarm2 (lte)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: lte.TestFailedAlarm2 Raised on class: lte.EPSPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when TestFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1024 TestFailedAlarm2 (rtr)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: rtr.TestFailedAlarm2 Raised on class: rtr.LDPTunnelInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1025 TestFailedAlarm2 (mpls)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: mpls.TestFailedAlarm2 Raised on class: mpls.P2MPDynamicLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1026 TestFailedAlarm2 (service)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: service.TestFailedAlarm2 Raised on class: service.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when TestFailedAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1027 TestFailedAlarm2 (svt)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: svt.TestFailedAlarm2 Raised on class: svt.SdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1027 TestFailedAlarm2 (svt) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1028 TestFailedAlarm2 (atm)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm2 (3739) Type: oamAlarm Package: atm.TestFailedAlarm2 Raised on class: atm.VPConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1029 TestFailedAlarm3 (svt)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm3 (3886) Type: oamAlarm Package: svt.TestFailedAlarm3 Raised on class: svt.SpokeSdpFec	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1030 TestFailedAlarm3 (service)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm3 (3886) Type: oamAlarm Package: service.TestFailedAlarm3 Raised on class: service.CompositeService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1031 TestFailedAlarm3 (mpls)

Alarm	Attributes	Applicable major release
Name: TestFailedAlarm3 (3886) Type: oamAlarm Package: mpls.TestFailedAlarm3 Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object fails.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1032 TestFailureAlarm

Alarm	Attributes	Applicable major release
Name: TestFailureAlarm (3903) Type: oamAlarm Package: sas.TestFailureAlarm Raised on class: sas.Test	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: This alarm is raised when a test failure trap is received from the node.		
Remedial action: Fix network connections issues.		

Table 39-1033 TestThresholdExceededAlarm (vlan)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: vlan.TestThresholdExceededAlarm Raised on class: vlan.Vlan	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1034 TestThresholdExceededAlarm (vll)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: vll.TestThresholdExceededAlarm Raised on class: vll.Vll	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		

Table 39-1034 TestThresholdExceededAlarm (vll) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1035 TestThresholdExceededAlarm (netw)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: netw.TestThresholdExceededAlarm Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1036 TestThresholdExceededAlarm (rtr)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: rtr.TestThresholdExceededAlarm Raised on class: rtr.VirtualRouter	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that the test threshold has been exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1037 TestThresholdExceededAlarm (service)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: service.TestThresholdExceededAlarm Raised on class: service.SpokeConnector	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1038 TestThresholdExceededAlarm (ethernetoam)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: ethernetoam.TestThresholdExceededAlarm Raised on class: ethernetoam.MaintAssociation	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1039 TestThresholdExceededAlarm (svt)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: svt.TestThresholdExceededAlarm Raised on class: svt.Tunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1040 TestThresholdExceededAlarm (lteservice)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: lteservice.TestThresholdExceededAlarm Raised on class: lteservice.MobileService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1041 TestThresholdExceededAlarm (mirror)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: mirror.TestThresholdExceededAlarm Raised on class: mirror.Mirror	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1041 TestThresholdExceededAlarm (mirror) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1042 TestThresholdExceededAlarm (ldp)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: ldp.TestThresholdExceededAlarm Raised on class: ldp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1043 TestThresholdExceededAlarm (bgp)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: bgp.TestThresholdExceededAlarm Raised on class: bgp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1044 TestThresholdExceededAlarm (monpath)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: monpath.TestThresholdExceededAlarm Raised on class: monpath.MonitoredIpPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1045 TestThresholdExceededAlarm (vpls)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: vpls.TestThresholdExceededAlarm Raised on class: vpls.AbstractVpls	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1046 TestThresholdExceededAlarm (lte)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: lte.TestThresholdExceededAlarm Raised on class: lte.EPSPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1047 TestThresholdExceededAlarm (atm)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: atm.TestThresholdExceededAlarm Raised on class: atm.PvcConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1048 TestThresholdExceededAlarm (mpls)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: mpls.TestThresholdExceededAlarm Raised on class: mpls.Lsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1048 TestThresholdExceededAlarm (mpls) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1049 TestThresholdExceededAlarm (vprn)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: vprn.TestThresholdExceededAlarm Raised on class: vprn.Vprn	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1050 TestThresholdExceededAlarm (pim)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: pim.TestThresholdExceededAlarm Raised on class: pim.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1051 TestThresholdExceededAlarm (mplstp)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm (1154) Type: oamAlarm Package: mplstp.TestThresholdExceededAlarm Raised on class: mplstp.TPLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1052 TestThresholdExceededAlarm2 (ethernetoam)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: ethernetoam.TestThresholdExceededAlarm2 Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that the test threshold has been exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1053 TestThresholdExceededAlarm2 (mpls)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: mpls.TestThresholdExceededAlarm2 Raised on class: mpls.P2MPDynamicLsp	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that the test threshold has been exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1054 TestThresholdExceededAlarm2 (atm)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: atm.TestThresholdExceededAlarm2 Raised on class: atm.VPConnection	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1055 TestThresholdExceededAlarm2 (rtr)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: rtr.TestThresholdExceededAlarm2 Raised on class: rtr.LDPTunnelInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A

Table 39-1055 TestThresholdExceededAlarm2 (rtr) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1056 TestThresholdExceededAlarm2 (service)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: service.TestThresholdExceededAlarm2 Raised on class: service.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1057 TestThresholdExceededAlarm2 (svt)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: svt.TestThresholdExceededAlarm2 Raised on class: svt.SdpBinding	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that the test threshold has been exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1058 TestThresholdExceededAlarm2 (lte)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm2 (1918) Type: oamAlarm Package: lte.TestThresholdExceededAlarm2 Raised on class: lte.EPSPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is un-reliable.		

Table 39-1059 TestThresholdExceededAlarm3 (mpls)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm3 (1919) Type: oamAlarm Package: mpls.TestThresholdExceededAlarm3 Raised on class: mpls.LspPath	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that a test threshold is exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1060 TestThresholdExceededAlarm3 (service)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm3 (1919) Type: oamAlarm Package: service.TestThresholdExceededAlarm3 Raised on class: service.CompositeService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when SasThresholdExceededAlarm is raised for any test on this object.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1061 TestThresholdExceededAlarm3 (svt)

Alarm	Attributes	Applicable major release
Name: TestThresholdExceededAlarm3 (1919) Type: oamAlarm Package: svt.TestThresholdExceededAlarm3 Raised on class: svt.SpokeSdpFec	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: networkDegradation	Release: • N/A
Description: The alarm is raised when an OAM test on the object reports that the test threshold has been exceeded.		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the underlying transport network is unreliable.		

Table 39-1062 ThresholdCrossingAlarm (netw)

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed Package: netw.ThresholdCrossingAlarm Raised on class: netw.NetworkElement	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A

Table 39-1062 ThresholdCrossingAlarm (netw) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a value crosses a configured rising or falling threshold. The alarm information includes the current threshold value, the default threshold value, and the threshold name.		
Remedial action: Informational - A TCA set in the statistics policy associated with the counter has fired. The counter in question should be examined to determine if further action is required.		

Table 39-1063 ThresholdCrossingAlarm (equipment)

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed Package: equipment.ThresholdCrossingAlarm Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a port value crosses a threshold.		
Remedial action: Informational - A TCA set in the statistics policy associated with the counter has fired. The counter in question should be examined to determine if further action is required.		

Table 39-1064 ThresholdCrossingAlarm (generic)

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed Package: generic.ThresholdCrossingAlarm Raised on class: generic.GenericObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a monitored object statistics-counter value exceeds a threshold value in the associated statistics policy.		
Remedial action: Informational - A TCA set in the statistics policy associated with the counter has fired. The counter in question should be examined to determine if further action is required.		

Table 39-1065 ThresholdCrossingAlarm (tca)

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarm (14) Type: thresholdCrossed Package: tca.ThresholdCrossingAlarm Raised on class: tca.SpecificTCAPolicy	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a monitored object statistics-counter value exceeds a threshold value in the associated statistics policy.		

Table 39-1065 ThresholdCrossingAlarm (tca) (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is generated when a threshold is crossed on an object or attribute supported by 5620 SAM. The object or attribute must be examined to determine the nature of the issue and the load on the entity must be examined to determine if it is appropriate.		

Table 39-1066 ThresholdCrossingAlarmCard

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmCard (2097) Type: thresholdCrossed Package: equipment.ThresholdCrossingAlarmCard Raised on class: equipment.BaseCard	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a card value crosses a TCA threshold.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 39-1067 ThresholdCrossingAlarmDbl

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmDbl (226) Type: thresholdCrossed Package: generic.ThresholdCrossingAlarmDbl Raised on class: generic.GenericObject	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a value crosses a configured rising or falling threshold. The alarm information includes the current threshold value, the default threshold value, and the threshold name.		
Remedial action: Informational - A TCA set in the statistics policy associated with the counter has fired. The counter in question should be examined to determine if further action is required.		

Table 39-1068 ThresholdCrossingAlarmOduk

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmOduk (4949) Type: thresholdCrossed Package: oth.ThresholdCrossingAlarmOduk Raised on class: oth.Oduk	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a ODUk value crosses a TCA threshold.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 39-1069 ThresholdCrossingAlarmOtuk

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmOtuk (4950) Type: thresholdCrossed Package: oth.ThresholdCrossingAlarmOtuk Raised on class: oth.Otuk	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a OTUk value crosses a TCA threshold.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 39-1070 ThresholdCrossingAlarmPort

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlarmPort (2098) Type: thresholdCrossed Package: equipment.ThresholdCrossingAlarmPort Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a port value crosses a TCA threshold.		
Remedial action: A condition set when a counter exceeds a user-selected high or low threshold. A TCA does not generate an alarm but is available on demand through the CIT.Please refer 1830 Troubleshooting guide for more details.		

Table 39-1071 ThresholdCrossingAlert

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingAlert (8407) Type: oamAlarm Package: sas.ThresholdCrossingAlert Raised on class: sas.PMSessionTest	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when a TCA is generated by the node.		
Remedial action: The alarm is raised if a sas pm test exceeds Threshold Limit.		

Table 39-1072 ThresholdCrossingMDAResvCBSAlarm

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingMDAResvCBSAlarm (3626) Type: thresholdCrossed Package: equipment. ThresholdCrossingMDAResvCBSAlarm Raised on class: equipment.DaughterCard	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A

Table 39-1072 ThresholdCrossingMDAResvCBSAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the reserved CBS of an MDA crosses a threshold.		
Remedial action: This alarm is raised when the traffic rates being received on an MDA are exceeding the amount of buffer allocated for the MDA in the committed burst size configuration parameter. In all probability the QoS being delivered by the MDA is degraded. Steps must be taken to shed traffic from the ports/links associated with the MDA.		

Table 39-1073 ThresholdCrossingPortResvCBSAlarm

Alarm	Attributes	Applicable major release
Name: ThresholdCrossingPortResvCBSAlarm (3627) Type: thresholdCrossed Package: equipment.ThresholdCrossingPortResvCBSAlarm Raised on class: equipment.PhysicalPort	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: thresholdCrossed	Release: • N/A
Description: The alarm is raised when the reserved CBS of a port crosses a threshold.		
Remedial action: This alarm is raised when the traffic rates being received on a port are exceeding the amount of buffer allocated for the port in the committed burst size configuration parameter. In all probability the QoS being delivered by the port is degraded. Steps must be taken to shed traffic from the port in question..		

Table 39-1074 TimedLicenseExpiryNotice

Alarm	Attributes	Applicable major release
Name: TimedLicenseExpiryNotice (263) Type: licensingAlarm Package: security.TimedLicenseExpiryNotice Raised on class: security.AbstractLicense	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: timedLicenseExpiryNotice	Release: • N/A
Description: The alarm is raised when the 5620 SAM license timer expires. The alarm information includes the license expiry date.		
Remedial action: Informational - The SAM license key is about to expire. Please contact your Nokia sales representative to request either an extension for the license or a permanent license key.		

Table 39-1075 TimeMismatch

Alarm	Attributes	Applicable major release
Name: TimeMismatch (436) Type: configurationAlarm Package: server.TimeMismatch Raised on class: server.AuxiliaryServer	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: timeMismatch	Release: • N/A
Description: The alarm is raised when the system time on a 5620 SAM auxiliary server station differs from the system time on a main server station.		

Table 39-1075 TimeMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The system time on the AUX server must match the system time on the main SAM server.		

Table 39-1076 TimeRefDisqualified

Alarm	Attributes	Applicable major release
Name: TimeRefDisqualified (8072) Type: communicationsAlarm Package: netw.TimeRefDisqualified Raised on class: netw.Time	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TimeRefDisqualified	Release: • N/A
Description: The alarm is raised when a system time input reference is disqualified.		
Remedial action: Informational- no corrective action required.		

Table 39-1077 TimeRefSelect

Alarm	Attributes	Applicable major release
Name: TimeRefSelect (8073) Type: communicationsAlarm Package: netw.TimeRefSelect Raised on class: netw.TimeSource	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: TimeRefSelect	Release: • N/A
Description: The alarm is raised when a system time input reference is selected.		
Remedial action: Informational - no corrective action required.		

Table 39-1078 TimingHoldover (equipment)

Alarm	Attributes	Applicable major release
Name: TimingHoldover (734) Type: communicationsAlarm Package: equipment.TimingHoldover Raised on class: equipment.ProcessorCard	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingHoldover	Release: • N/A
Description: The alarm is raised when the Standby CPM goes into or out of Timing holdover state.		
Remedial action: Informational only.		

Table 39-1079 TimingHoldover (sonet)

Alarm	Attributes	Applicable major release
Name: TimingHoldover (734) Type: communicationsAlarm Package: sonet.TimingHoldover Raised on class: sonet.SiteSync	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingHoldover	Release: • N/A
Description: The alarm is raised when the timing of an NE is in the Holdover state.		
Raising condition: (('Status' EQUAL 'Master Holdover'))		
Clearing condition: (('Status' NOT EQUAL 'Master Holdover'))		
Remedial action: Informational only.		

Table 39-1080 TimingReferenceOneNotQualified

Alarm	Attributes	Applicable major release
Name: TimingReferenceOneNotQualified (545) Type: communicationsAlarm Package: sonet.TimingReferenceOneNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • N/A
Description: The alarm is raised when Timing Reference One on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that Timing Reference One is qualified.		

Table 39-1081 TimingReferenceTwoNotQualified

Alarm	Attributes	Applicable major release
Name: TimingReferenceTwoNotQualified (546) Type: communicationsAlarm Package: sonet.TimingReferenceTwoNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • N/A
Description: The alarm is raised when Timing Reference Two on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that Timing Reference Two is qualified.		

Table 39-1082 TMNLossofSignal (mpr)

Alarm	Attributes	Applicable major release
Name: TMNLossofSignal (1920) Type: communicationsAlarm Package: mpr.TMNLossofSignal Raised on class: mpr.MprTMN	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tmnLOS	Release: • N/A
Description: The alarm is raised when a Loss of Signal occurs on the TMN Interface.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-1083 TmnxBsxUrlListFailure

Alarm	Attributes	Applicable major release
Name: TmnxBsxUrlListFailure (8374) Type: processingErrorAlarm Package: aapolicy.TmnxBsxUrlListFailure Raised on class: aapolicy.AAUrlListPolicy	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TmnxBsxUrlListFailure	Release: • N/A
Description: This alarm is generated when a URL list has failed.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('isLocal' EQUAL 'true'))		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: The URL list has failed. Ensure the correct file is configured in the File URL. Administratively disable and re-enable or use CLI command 'upgrade' to restart the URL List.		

Table 39-1084 TmnxBsxUrlListUpdate

Alarm	Attributes	Applicable major release
Name: TmnxBsxUrlListUpdate (8375) Type: processingErrorAlarm Package: aapolicy.TmnxBsxUrlListUpdate Raised on class: aapolicy.AAUrlListPolicy	Severity: info Specific problem: Not Applicable Implicitly cleared: false Default probable cause: TmnxBsxUrlListUpdate	Release: • N/A
Description: This alarm is generated when a URL list has been updated.		
Remedial action: Informational - The URL list has been updated. No corrective action required.		

Table 39-1085 tmnxMcSyncClientAlarm

Alarm	Attributes	Applicable major release
Name: tmnxMcSyncClientAlarm (423) Type: communicationsAlarm Package: multichassis.tmnxMcSyncClientAlarm Raised on class: multichassis.PeerSynchronizationProtocol	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: locallyDeletedEntryInMCSync-Database	Release: • N/A
Description: The alarm is raised when a MC synchronization database entry is deleted locally.		
Remedial action: Informational only.		

Table 39-1086 TodSuiteAssignmentFailure (service)

Alarm	Attributes	Applicable major release
Name: TodSuiteAssignmentFailure (312) Type: todSuiteAlarm Package: service.TodSuiteAssignmentFailure Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: configConflictOrResourceFull	Release: • N/A
Description: The alarm is raised when a Time of Day suite cannot be assigned to an aggregation scheduler, or to an L2 or L3 access interface, because of a configuration conflict or a lack of resources. The alarm is not raised against a SAP.		
Remedial action: A configuration error has been made which must be corrected. The TOD cannot be assigned to the Aggregation Scheduler due to a configuration conflict or lack of resources.		

Table 39-1087 TodSuiteAssignmentFailure (svq)

Alarm	Attributes	Applicable major release
Name: TodSuiteAssignmentFailure (312) Type: todSuiteAlarm Package: svq.TodSuiteAssignmentFailure Raised on class: svq.AggregationScheduler	Severity: minor Specific problem: Not Applicable Implicitly cleared: false Default probable cause: assignmentFailure	Release: • N/A
Description: The alarm is raised when an object fails to perform the action specified in a Time of Day suite.		
Remedial action: A configuration error has been made which must be corrected. The TOD cannot be assigned to the Aggregation Scheduler due to a configuration conflict or lack of resources.		

Table 39-1088 TooManyCpaaPerIsisArea

Alarm	Attributes	Applicable major release
Name: TooManyCpaaPerIsisArea (385) Type: configurationAlarm Package: topology.TooManyCpaaPerIsisArea Raised on class: topology.Cpaa	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tooManyCpaaPeIsisArea	Release: • N/A

Table 39-1088 TooManyCpaaPerIsisArea (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when there are too many 7701 CPAAs for an ISIS L1 area.		
Remedial action: Check the configuration of CPAA and make sure there is at most one CPAA configured for an ISIS area within an administrative domain.		

Table 39-1089 TopologyIsisSystemError

Alarm	Attributes	Applicable major release
Name: TopologyIsisSystemError (373) Type: topologyAlarm Package: topology.TopologyIsisSystemError Raised on class: topology.AutonomousSystem	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: isisSystemNotAdvertisingTeR-outerId	Release: • N/A
Description: The alarm is raised when an IS-IS topology system error is detected.		
Remedial action: Alarm contains the systemId of the router which is not advertising ISIS TE RouterId. User should either configure the ISIS TE routerId on the node or configure a routerId for that system in "ISIS System ID Mapping" menu. Configuring the routerId in systemID mapping will not clear the alarm.		

Table 39-1090 TopologyMisconfigured

Alarm	Attributes	Applicable major release
Name: TopologyMisconfigured (95) Type: configurationAlarm Package: service.TopologyMisconfigured Raised on class: service.Service	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • N/A
Description: This alarm is raised when service sites are not fully connected.		
Raising condition: ('topologyMisconfigured' EQUAL 'true')		
Clearing condition: ('topologyMisconfigured' EQUAL 'false')		
Remedial action: Connect the service sites with SDP Bindings, Vlan Uplinks, or PBB tunnels.		

Table 39-1091 topologyMisconfigured

Alarm	Attributes	Applicable major release
Name: topologyMisconfigured (11467) Type: communicationsAlarm Package: mpr.topologyMisconfigured Raised on class: mpr.BackhaulService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • N/A
Description: The alarm is raised when any configuration mismatch are present in a service.		

Table 39-1091 topologyMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Topology Misconfigured' EQUAL 'true')		
Clearing condition: ('Topology Misconfigured' EQUAL 'false')		
Remedial action: Check for any configuration mismatch in the physical topology.		

Table 39-1092 TopologyRuleExecutionError

Alarm	Attributes	Applicable major release
Name: TopologyRuleExecutionError (365) Type: configurationAlarm Package: tunnelmgmt.TopologyRuleExecutionError Raised on class: tunnelmgmt.TopologyRule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: ruleErrorOrRuleEngineError	Release: • N/A
Description: The alarm is raised when the 5620 SAM cannot execute a topology rule or when rule execution generates an error. Rule execution is the process that determines which tunnel elements require creation, modification, or deletion. The alarm typically indicates that the rule is misconfigured.		
Remedial action: A configuration error has been made which must be corrected. The topology rule in question must be re-configured correctly.		

Table 39-1093 TraceError

Alarm	Attributes	Applicable major release
Name: TraceError (289) Type: equipmentAlarm Package: netw.TraceError Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: traceError	Release: • N/A
Description: The alarm is raised when unusual error log trace messages are generated on an NE. The alarm information includes the title of the logged event and message details.		
Remedial action: Informational - This alarm is generated by the SR platforms to indicate that the node has encountered a reportable problem. The additional text field of the alarm will contain additional information regarding the alarm. If the alarm persists please contact your Nokia support representative for assistance.		

Table 39-1094 TrafficElectricalEthernetLinkDown

Alarm	Attributes	Applicable major release
Name: TrafficElectricalEthernetLinkDown (8401) Type: communicationsAlarm Package: mwa.TrafficElectricalEthernetLinkDown Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • N/A
Description: The alarm is raised when the electrical ethernet link goes down.		

Table 39-1094 TrafficElectricalEthernetLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-1095 TrafficOpticalEthernetLinkDown

Alarm	Attributes	Applicable major release
Name: TrafficOpticalEthernetLinkDown (8971) Type: communicationsAlarm Package: mwa.TrafficOpticalEthernetLinkDown Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • N/A
Description: The alarm is raised when the optical ethernet link goes down.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-1096 TrafficPortSFPCardFail

Alarm	Attributes	Applicable major release
Name: TrafficPortSFPCardFail (8972) Type: equipmentAlarm Package: mwa.TrafficPortSFPCardFail Raised on class: mwa.PortTermination	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitProblem	Release: • N/A
Description: The alarm is raised when a MPT detects a traffic port SFP card failure.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-1097 TrafficPortSFPMissing

Alarm	Attributes	Applicable major release
Name: TrafficPortSFPMissing (8973) Type: equipmentAlarm Package: mwa.TrafficPortSFPMissing Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReplaceableUnitMissing	Release: • N/A
Description: This alarm is raised when traffic port SFP is missing.		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-1098 TrailDegrade

Alarm	Attributes	Applicable major release
Name: TrailDegrade (8101) Type: communicationsAlarm Package: optical.TrailDegrade Raised on class: optical.Trail	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionDegrade	Release: • N/A
Description: The alarm is raised when either Trail Path of Protected Trail is Operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on APS Group's work and protect TPs to understand why trail protection is degraded.		

Table 39-1099 TrailPathDown

Alarm	Attributes	Applicable major release
Name: TrailPathDown (5128) Type: communicationsAlarm Package: optical.TrailPathDown Raised on class: optical.TrailPath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the trail path are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-1100 TrailSignalFail

Alarm	Attributes	Applicable major release
Name: TrailSignalFail (798) Type: communicationsAlarm Package: bundle.TrailSignalFail Raised on class: bundle.Interface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trailSignalFailure	Release: • N/A
Description: The alarm is raised when a a local or remote failure in an IMA group generates a Trail Signal Fail message.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-1101 TransportServerDegrade

Alarm	Attributes	Applicable major release
Name: TransportServerDegrade (10268) Type: communicationsAlarm Package: optical.TransportServerDegrade Raised on class: optical.TransportService	Severity: cleared Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnderlyingServerDegraded	Release: • N/A
Description: The alarm is raised when any of the underlying protected server trail in the service is degraded		

Table 39-1101 TransportServerDegrade (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on Server Trails to understand why trail protection is unreliable.		

Table 39-1102 TransportServerFailure

Alarm	Attributes	Applicable major release
Name: TransportServerFailure (8104) Type: communicationsAlarm Package: optical.TransportServerFailure Raised on class: optical.TransportService	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnderlyingServerDown	Release: • N/A
Description: The alarm is raised when any of the server trails in the service is operationally down		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on Server Trails to understand why transport service protection is unreliable.		

Table 39-1103 TransportServiceDegrade

Alarm	Attributes	Applicable major release
Name: TransportServiceDegrade (8105) Type: communicationsAlarm Package: optical.TransportServiceDegrade Raised on class: optical.TransportService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ProtectionDegrade	Release: • N/A
Description: The alarm is raised when either work or protect path of Protected Transport Service is operationally down		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on APS Group's work and protect TPs to understand why transport service protection is degraded.		

Table 39-1104 TransportServiceDown

Alarm	Attributes	Applicable major release
Name: TransportServiceDown (2906) Type: communicationsAlarm Package: optical.TransportServiceDown Raised on class: optical.TransportService	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when: 1. The termination point(s) or VTS XC's of the service path(s) are operationally down. 2. There are missing VTS XCs in any of the service path(s) of this transport service.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-1105 TransportServicePathDown

Alarm	Attributes	Applicable major release
Name: TransportServicePathDown (4402) Type: communicationsAlarm Package: optical.TransportServicePathDown Raised on class: optical.ServicePath	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OperationalStateDown	Release: • N/A
Description: The alarm is raised when the termination point(s) of the service path are operationally down.		
Remedial action: Informational - If the alarm persists or is occurring frequently then investigation is required by looking at the active alarms on the hops to understand why the underlying transport network is unreliable.		

Table 39-1106 TrapMalformed

Alarm	Attributes	Applicable major release
Name: TrapMalformed (135) Type: communicationsAlarm Package: netw.TrapMalformed Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapSchemaMismatch	Release: • N/A
Description: The alarm is raised when the number of varbinds in an incoming SNMP trap is fewer than the number expected.		
Remedial action: Informational - If the alarm persists please contact your Nokia support representative for assistance		

Table 39-1107 TrapMapperQueueFull

Alarm	Attributes	Applicable major release
Name: TrapMapperQueueFull (797) Type: queueFull Package: trapmapper.TrapMapperQueueFull Raised on class: trapmapper.TrapMapperManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapRateTooHigh	Release: • N/A
Description: The alarm is raised when the 5620 SAM detects that the queue for traps that are to be mapped to alarms is full. Until queue space is available, the 5620 SAM drops traps that are to be mapped to alarms.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

Table 39-1108 TrapRateThresholdExceeded

Alarm	Attributes	Applicable major release
Name: TrapRateThresholdExceeded (412) Type: communicationsAlarm Package: netw.TrapRateThresholdExceeded Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapRateGreaterThanConfig-ured	Release: • N/A

Table 39-1108 TrapRateThresholdExceeded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the incoming SNMP trap rate is greater than the configured trap rate threshold.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

Table 39-1109 TunnelElementCreationError

Alarm	Attributes	Applicable major release
Name: TunnelElementCreationError (366) Type: configurationAlarm Package: tunnelmgmt.TunnelElementCreationError Raised on class: tunnelmgmt.TopologyRule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unableToCreateTunnelElement	Release: • N/A
Description: The alarm is raised when the creation of a missing tunnel element fails.		
Remedial action: A configuration error has been made which must be corrected. Please resolve the configuration error preventing the creation of the tunnel element.		

Table 39-1110 TunnelElementDeleteError

Alarm	Attributes	Applicable major release
Name: TunnelElementDeleteError (367) Type: configurationAlarm Package: tunnelmgmt.TunnelElementDeleteError Raised on class: tunnelmgmt.TopologyRule	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tunnelElementInUse	Release: • N/A
Description: The alarm is raised when the deletion of an obsolete or unused tunnel element fails.		
Remedial action: A configuration error has occurred which must be corrected. The correction of this error must be done via CLI - please log into the NE and delete the tunnel element.		

Table 39-1111 TunnelElementInUseWarning

Alarm	Attributes	Applicable major release
Name: TunnelElementInUseWarning (368) Type: configurationAlarm Package: tunnelmgmt.TunnelElementInUseWarning Raised on class: tunnelmgmt.TopologyRule	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tunnelElementInUse	Release: • N/A
Description: The alarm is raised when the 5620 SAM does not attempt to delete an obsolete or unused tunnel element because the element is in use by another object.		
Remedial action: A configuration error has been made which must be corrected. The tunnel object to be deleted must be removed from the service or services which are referring to it.		

Table 39-1112 TunnelOverbooked

Alarm	Attributes	Applicable major release
Name: TunnelOverbooked (590) Type: resourceAlarm Package: svt.TunnelOverbooked Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tunnelOverbooked	Release: • N/A
Description: The alarm is raised when the allocated SDP binding bandwidth specified by sdpBookedBandwidth exceeds the sdpMaxBookableBandwidth value.		
Clearing condition: ('SDP Available Bandwidth' NOT EQUAL '0')		
Remedial action: Please set the maximum bookable bandwidth parameter to a more appropriate value or offload traffic from the SDP in question to another SDP.		

Table 39-1113 TunnelSelBlacklistFull

Alarm	Attributes	Applicable major release
Name: TunnelSelBlacklistFull (4626) Type: processingErrorAlarm Package: l2tp.TunnelSelBlacklistFull Raised on class: l2tp.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tmnxL2tpTunnelSelBlacklistFull	Release: • N/A
Description: This alarm is raised when the number of tunnels and peers in the tunnel-selection-blacklist reaches the limit configured on the L2TP Site, and is cleared when the limit is no longer reached.		
Remedial action: Either increase Max List Length in Tunnel Selection Blacklist configuration or fix blacklisted tunnels or peers.		

Table 39-1114 TwampReflectorAlarm

Alarm	Attributes	Applicable major release
Name: TwampReflectorAlarm (8138) Type: oamAlarm Package: sas.TwampReflectorAlarm Raised on class: sas.TWLSession	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingTwlReflectorConfiguration	Release: • N/A
Description: This alarm is raised when a Twamp-Light Session is configured without a matching Reflector Prefix.		
Remedial action: This alarm is raised when a Twamp-Light Session is configured without a matching Reflector Prefix.		

Table 39-1115 TwampSrvInactivityTimeout

Alarm	Attributes	Applicable major release
Name: TwampSrvInactivityTimeout (3319) Type: communicationsAlarm Package: sas.TwampSrvInactivityTimeout Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPServerInactivityTimeout	Release: • N/A
Description: The alarm is raised when a TWAMP control connection is disconnected by the TWAMP server due to the connection being inactive for a period exceeding the server's inactivity timeout, which generates a TWAMP Server InactivityTimeout notification.		
Remedial action: Verify the value of the inactivity-timeout parameter and modify it according to the operational needs.		

Table 39-1116 TwampSrvMaxConnsExceeded

Alarm	Attributes	Applicable major release
Name: TwampSrvMaxConnsExceeded (3320) Type: communicationsAlarm Package: sas.TwampSrvMaxConnsExceeded Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPServerMaxConnsExceeded	Release: • N/A
Description: The alarm is raised when the maximum number of concurrent TWAMP control connections for the server has been reached. [EFFECT] The TWAMP client cannot request test runs on the rejected connection. [RECOVERY] Configure the system-level maximum number of concurrent TWAMP control connections to a larger value, or disconnect any TWAMP control connection.'		
Remedial action: Verify the value of the max-conn-server parameter and modify it according to the operational needs.		

Table 39-1117 TwampSrvMaxSessExceeded

Alarm	Attributes	Applicable major release
Name: TwampSrvMaxSessExceeded (3321) Type: communicationsAlarm Package: sas.TwampSrvMaxSessExceeded Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPServerMaxSessExceeded	Release: • N/A
Description: The alarm is raised when the maximum number of concurrent TWAMP sessions for the server has been reached. [EFFECT] The TWAMP client cannot request test runs on the rejected session. [RECOVERY] Configure the system-level maximum number of concurrent TWAMP sessions to a larger value, or disconnect any TWAMP session.'		
Remedial action: Verify the max-sess-server parameter and modify it according to the operational needs.		

Table 39-1118 TwampSrvPfxMaxConnsExceeded

Alarm	Attributes	Applicable major release
Name: TwampSrvPfxMaxConnsExceeded (3322) Type: communicationsAlarm Package: sas.TwampSrvPfxMaxConnsExceeded Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPServerPrefixxMax-ConnsExceeded	Release: • N/A
Description: The alarm is raised when the maximum number of concurrent TWAMP control connections for a TWAMP client prefix has been reached. [EFFECT] The TWAMP client cannot request test runs on the rejected connection. [RECOVERY] Configure the prefix's maximum number of concurrent TWAMP control connections to a larger value, or disconnect a TWAMP control connection which uses the prefix.		
Remedial action: Verify the max-conn-prefix parameter and modify it according to the operational needs.		

Table 39-1119 TwampSrvPfxMaxSessExceeded

Alarm	Attributes	Applicable major release
Name: TwampSrvPfxMaxSessExceeded (3323) Type: communicationsAlarm Package: sas.TwampSrvPfxMaxSessExceeded Raised on class: sas.TwampSrv	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: TWAMPServerPrefixMaxSes-sExceeded	Release: • N/A
Description: The alarm is raised when the maximum number of concurrent TWAMP sessions for a TWAMP client prefix has been reached. [EFFECT] The TWAMP client cannot request test runs on the rejected session. [RECOVERY] Configure the prefix's maximum number of concurrent TWAMP sessions to a larger value, or disconnect a TWAMP session which uses the prefix.'		
Remedial action: Verify the max sess-prefix parameter and modify it according to the operational needs.		

Table 39-1120 TwoPrimaryDatabase

Alarm	Attributes	Applicable major release
Name: TwoPrimaryDatabase (202) Type: configurationAlarm Package: db.TwoPrimaryDatabase Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: twoPrimaryDatabase	Release: • N/A
Description: The alarm is raised when the standby database initializes as a primary database because of a database failover. The alarm clears when the original primary database is operational as the new standby database.		
Remedial action: Informational - The root cause of the failure of the primary database server should be investigated. Possible causes include a HW failure on the platform hosting the database function, loss of network connectivity between the primary and standby database.		

Table 39-1121 TxFail

Alarm	Attributes	Applicable major release
Name: TxFail (1175) Type: communicationsAlarm Package: equipment.TxFail Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txFail	Release: • N/A
Description: The alarm is raised when a transmission failure is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-1122 TxFailure

Alarm	Attributes	Applicable major release
Name: TxFailure (3931) Type: communicationsAlarm Package: equipment.TxFailure Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: txFail	Release: • N/A
Description: The alarm is raised when a txFail (a fail of the Tx subfunction) defect raise.		
Remedial action: The alarm is raised when a txFail (a fail of the Tx subfunction) defect raise.		

Table 39-1123 TxRetransmit

Alarm	Attributes	Applicable major release
Name: TxRetransmit (266) Type: communicationsAlarm Package: ospf.TxRetransmit Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hello Applicable probable causes: • hello • dbDescript • lsReq • lsUpdate • lsAck • nullPacket	Release: • N/A
Description: The alarm is raised when an NE retransmits an OSPF packet on a non-virtual interface. The alarm information includes the NE ID of the OSPF neighbor.		
Remedial action: Informational - an NE retransmits an OSPF packet on a non-virtual interface. The alarm information includes the NE ID of the OSPF neighbor.		

Table 39-1124 TypeMismatch

Alarm	Attributes	Applicable major release
Name: TypeMismatch (96) Type: configurationAlarm Package: service.TypeMismatch Raised on class: service.Service	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: serviceSiteTypeMisconfigured	Release: • N/A
Description: The alarm is raised when a VLAN type for a Site doesn't match what has been configured on the Service.		
Raising condition: ('serviceTypeInconsistent' EQUAL 'true')		
Clearing condition: ('serviceTypeInconsistent' EQUAL 'false')		
Remedial action: Configure the VLAN subtype on the site same as the service VLAN subtype.		

Table 39-1125 UnableDeleteArchivedLogs

Alarm	Attributes	Applicable major release
Name: UnableDeleteArchivedLogs (200) Type: databaseAlarm Package: db.UnableDeleteArchivedLogs Raised on class: db.DatabaseManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: archivedLogsIssue	Release: • N/A
Description: The alarm is raised when database disk space is low and the 5620 SAM is unable to delete the archive logs.		
Remedial action: Informational - Please contact your Nokia support representative for assistance.		

Table 39-1126 UnableGetArchivedLogDiskInfo

Alarm	Attributes	Applicable major release
Name: UnableGetArchivedLogDiskInfo (4976) Type: databaseAlarm Package: db.UnableGetArchivedLogDiskInfo Raised on class: db.DatabaseManager	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: archivedLogsIssue	Release: • N/A
Description: The alarm is raised when the 5620 SAM is unable to get the archive log filesystem information.		
Remedial action: Informational - Please check archive logs file system. The 5620 SAM cannot access the file system. If the problem persists then please contact your Nokia support representative for assistance.		

Table 39-1127 UnavailableTime

Alarm	Attributes	Applicable major release
Name: UnavailableTime (644) Type: communicationsAlarm Package: equipment.UnavailableTime Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unavailableTime	Release: • N/A

Table 39-1127 UnavailableTime (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a port experiences 10 consecutive SES.		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 39-1128 UnavailableTimeHigherOrderVCPath

Alarm	Attributes	Applicable major release
Name: UnavailableTimeHigherOrderVCPath (9009) Type: communicationsAlarm Package: tdm.UnavailableTimeHigherOrderVCPath Raised on class: tdm.AUn	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UATHOVC	Release: • N/A
Description: The alarm is raised on Unavailable Time, Higher Order VC path (NEND).		
Remedial action: Unavailable Time, Higher Order VC path (NEND).		

Table 39-1129 UnconfiguredEquipmentPresent

Alarm	Attributes	Applicable major release
Name: UnconfiguredEquipmentPresent (645) Type: equipmentAlarm Package: equipment.UnconfiguredEquipmentPresent Raised on class: equipment.Equipment	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unconfiguredEquipmentPresent	Release: • N/A
Description: The alarm is raised when unconfigured equipment is detected.		
Remedial action: A configuration error has occurred which must be corrected. The card slot has not been configured		

Table 39-1130 UndefinedSchedulerReference

Alarm	Attributes	Applicable major release
Name: UndefinedSchedulerReference (118) Type: configurationAlarm Package: vs.UndefinedSchedulerReference Raised on class: vs.ServiceTypeDefinition	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: undefinedSchedulerReference	Release: • N/A
Description: The alarm is raised when a queue specified in the access ingress or access egress policy of an L2 access interface is not referenced by the scheduler policy for the interface.		
Raising condition: (('numberReferences' > '0') AND ('numberOfDefinitions' EQUAL '0'))		

Table 39-1130 UndefinedSchedulerReference (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('numberReferences' EQUAL '0') OR ('numberOfDefinitions' > '0'))		
Remedial action: A queue specified in the access ingress/egress policy used by an L2 access interface is not referencing a scheduler policy. Ensure all required queues created in the access ingress/egress policy is referencing a scheduler.		

Table 39-1131 UnderlyingResourceDegrade

Alarm	Attributes	Applicable major release
Name: UnderlyingResourceDegrade (1176) Type: communicationsAlarm Package: equipment.UnderlyingResourceDegrade Raised on class: equipment.Port	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceDegrade	Release: • N/A
Description: The alarm is raised when degradation of an underlying radio interface resource is detected.		
Remedial action: Please refer to the 9500 Node Maintenance manual for remedial action information.		

Table 39-1132 UnknownKeyGroupKeysDetected (nge)

Alarm	Attributes	Applicable major release
Name: UnknownKeyGroupKeysDetected (8977) Type: configurationAlarm Package: nge.UnknownKeyGroupKeysDetected Raised on class: nge.KeyGroup	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • N/A
Description: The alarm is raised when Key Group Keys are detected that were not created by NGE Manager.		
Remedial action: Check for similar alarms on the Network Element or KeyGroup objects, and take the action specified.		

Table 39-1133 UnknownNGEInstancesDetected

Alarm	Attributes	Applicable major release
Name: UnknownNGEInstancesDetected (8997) Type: configurationAlarm Package: nge.UnknownNGEInstancesDetected Raised on class: nge. NetworkGroupEncryptionManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • N/A
Description: The alarm is raised when Group Encryption configurations are detected which were not created by NGE Manager.		
Remedial action: Look for alarms on individual security objects and take appropriate action.		

Table 39-1134 UnknownSDPKeyGroupIdDetected (svt)

Alarm	Attributes	Applicable major release
Name: UnknownSDPKeyGroupIdDetected (8978) Type: configurationAlarm Package: svt.UnknownSDPKeyGroupIdDetected Raised on class: svt.Tunnel	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: UnknownNGEConfiguration	Release: • N/A
Description: The alarm is raised when a Key Group Id is configured on an SDP which was not configured by NGE manager.		
Remedial action: Remove encryption configuration for this SDP from node CLI.		

Table 39-1135 UnmanagedMplsTpSDPTunnelSite

Alarm	Attributes	Applicable major release
Name: UnmanagedMplsTpSDPTunnelSite (8147) Type: configurationAlarm Package: svt.UnmanagedMplsTpSDPTunnelSite Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unmanagedMplsTpSDPTunnelSite	Release: • N/A
Description: The alarm is raised when the MPLS-TP SDP Tunnel has configured with a non-managed site.		
Remedial action: Investigation is required to resolve the following possible scenarios: The far-end site at the MPLS-TP SDP Tunnel is non-managed Site. Please start to manage the NE with SAM or change the far-end site id to a correct MPLS-TP site at MPLS-TP SDP Tunnel form.		

Table 39-1136 UNREGISTERED_ALARM (racfl)

Alarm	Attributes	Applicable major release
Name: UNREGISTERED_ALARM (11596) Type: processingErrorAlarm Package: racfl.UNREGISTERED_ALARM Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: UNREGISTERED ALARM Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • N/A
Description: UNREGISTERED ALARM		
Remedial action: Contact Nokia support team for additional information if the problem persists.		

Table 39-1137 UNREGISTERED_ALARM (racloms)

Alarm	Attributes	Applicable major release
Name: UNREGISTERED_ALARM (11596) Type: processingErrorAlarm Package: racloms.UNREGISTERED_ALARM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNREGISTERED ALARM Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • N/A

Table 39-1137 UNREGISTERED_ALARM (racloms) (continued)

Alarm	Attributes	Applicable major release
Description: UNREGISTERED ALARM		
Remedial action: Contact Nokia support team for additional information if the problem persists.		

Table 39-1138 UnresolvedVirtualPortConfiguration

Alarm	Attributes	Applicable major release
Name: UnresolvedVirtualPortConfiguration (4908) Type: virtualPortAlarm Package: dctr.UnresolvedVirtualPortConfiguration Raised on class: dctr.AbstractVirtualPort	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UnableToResolveNetwork-Configuration	Release: • N/A
Description: The alarm is raised when VSD was not able to resolve network configuration for this virtual port. The virtual port will not be assigned an ip address and there is no service associated with it.		
Remedial action: This alarm can be cleared when VSD is able to resolve the network configuration of the virtual port. This notification reports that VSD cannot assign service objects to this virtual port. This could be one or more of the domain, zone, subnet, user, or permission are missing, mismatched or not properly configured in VSD. Please make sure the settings in VSD are correct for this virtual port.		

Table 39-1139 UnsupportedNode

Alarm	Attributes	Applicable major release
Name: UnsupportedNode (288) Type: configurationAlarm Package: netw.UnsupportedNode Raised on class: netw.Topology	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: unsupportedNode	Release: • N/A
Description: The alarm is raised when, during network discovery, the 5620 SAM detects an NE that uses an unsupported device software version. The alarm information includes the IP address of the NE.		
Remedial action: The SW version of the NE must be upgraded to a version supported by 5620 SAM.		

Table 39-1140 UserSuspended

Alarm	Attributes	Applicable major release
Name: UserSuspended (1123) Type: communicationsAlarm Package: security.UserSuspended Raised on class: security.User	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: multipleSecurityViolations	Release: • N/A
Description: The alarm is raised when a user account is suspended.		

Table 39-1140 UserSuspended (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - the user is suspended due to either a) the user account has been dormant longer than system's age threshold for account expiry, b) the password for the user has expired, or c) the number of authentication failures threshold before lockout has been reached.		

Table 39-1141 VirtualLinkDbDescriptAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkDbDescriptAuthFailure (61) Type: authenticationAlarm Package: ospf.VirtualLinkDbDescriptAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a dbDescript packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a virtual link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1142 VirtualLinkDbDescriptConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkDbDescriptConfig (55) Type: configurationAlarm Package: ospf.VirtualLinkDbDescriptConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a dbDescript packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a dbDescript packet has been received on a virtual link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-1143 VirtualLinkHelloAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkHelloAuthFailure (60) Type: authenticationAlarm Package: ospf.VirtualLinkHelloAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a virtual link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1144 VirtualLinkHelloConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkHelloConfig (54) Type: configurationAlarm Package: ospf.VirtualLinkHelloConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a hello packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a hello packet has been received on a virtual link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-1145 VirtualLinkLsAckAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsAckAuthFailure (64) Type: authenticationAlarm Package: ospf.VirtualLinkLsAckAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a virtual link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1146 VirtualLinkLsAckConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsAckConfig (58) Type: configurationAlarm Package: ospf.VirtualLinkLsAckConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsAck packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsAck packet has been received on a virtual link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-1147 VirtualLinkLsReqAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsReqAuthFailure (62) Type: authenticationAlarm Package: ospf.VirtualLinkLsReqAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a virtual link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1148 VirtualLinkLsReqConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsReqConfig (56) Type: configurationAlarm Package: ospf.VirtualLinkLsReqConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsReq packet has been received on a virtual link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-1149 VirtualLinkLsUpdateAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsUpdateAuthFailure (63) Type: authenticationAlarm Package: ospf.VirtualLinkLsUpdateAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives an lsReq packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a virtual link from the network whose authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1150 VirtualLinkLsUpdateConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkLsUpdateConfig (57) Type: configurationAlarm Package: ospf.VirtualLinkLsUpdateConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives an lsUpdate packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a lsUpdate packet has been received on a virtual link from the network whose configuration parameters conflict with the local NE's configurations.		

Table 39-1151 VirtualLinkNullPacketAuthFailure

Alarm	Attributes	Applicable major release
Name: VirtualLinkNullPacketAuthFailure (65) Type: authenticationAlarm Package: ospf.VirtualLinkNullPacketAuthFailure Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: authTypeMismatch Applicable probable causes: • authTypeMismatch • authFailure	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a virtual link from an NE whose authentication key or authentication type conflicts with the local NE authentication key or authentication type.		
Remedial action: Informational - The alarm signifies that a null packet has been received on a virtual link which authentication key or authentication type conflicts with the local NE's configuration.		

Table 39-1152 VirtualLinkNullPacketConfig

Alarm	Attributes	Applicable major release
Name: VirtualLinkNullPacketConfig (59) Type: configurationAlarm Package: ospf.VirtualLinkNullPacketConfig Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: badVersion Applicable probable causes: • badVersion • areaMismatch • unknownNbmaNbr • unknownVirtualNbr • netMaskMismatch • helloIntervalMismatch • deadIntervalMismatch • optionMismatch • mtuMismatch • noError • duplicateRouterId • ifAdminDown • ifPassive	Release: • N/A
Description: The alarm is raised when an NE receives a null packet on a virtual link from an NE whose configuration parameters conflict with the local NE configuration parameters.		
Remedial action: Informational - The alarm signifies that a null packet has been received on a virtual link which configuration parameters conflict with the local NE's configurations.		

Table 39-1153 VirtualLinkRxBadPacket

Alarm	Attributes	Applicable major release
Name: VirtualLinkRxBadPacket (66) Type: communicationsAlarm Package: ospf.VirtualLinkRxBadPacket Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: false Default probable cause: hello Applicable probable causes: • hello • dbDescript • lsReq • lsUpdate • lsAck • nullPacket	Release: • N/A
Description: The alarm is raised when an NE cannot parse an OSPF packet that it receives on a virtual interface.		

Table 39-1153 VirtualLinkRxBadPacket (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - an NE cannot parse an OSPF packet that it receives on a virtual interface.		

Table 39-1154 VirtualMachineDown

Alarm	Attributes	Applicable major release
Name: VirtualMachineDown (4909) Type: vmAlarm Package: dctr.VirtualMachineDown Raised on class: dctr.VirtualMachine	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualMachineShutDownOr-DeletedOrCrashed	Release: • N/A
Description: The alarm is raised when VM is shutdown.		
Remedial action: This alarm can be cleared when virtual machine is up.		

Table 39-1155 VirtualMachineSuspended

Alarm	Attributes	Applicable major release
Name: VirtualMachineSuspended (4911) Type: vmAlarm Package: dctr.VirtualMachineSuspended Raised on class: dctr.VirtualMachine	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: UserInitiatatedOrRequire-dResourceIdBeingBlocked	Release: • N/A
Description: The alarm is raised when VM state changes to Paused on this object.		
Raising condition: (('Virtual Machine State' EQUAL 'Paused'))		
Clearing condition: (('Virtual Machine State' NOT EQUAL 'Paused'))		
Remedial action: This alarm can be cleared when the virtual machine is resumed.		

Table 39-1156 VirtualPortDown

Alarm	Attributes	Applicable major release
Name: VirtualPortDown (5434) Type: virtualPortAlarm Package: dctr.VirtualPortDown Raised on class: dctr.AbstractVirtualPort	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualPortDownOrDeleted	Release: • N/A
Description: The alarm is raised when VP is shutdown.		
Remedial action: This alarm can be cleared when virtual port is up.		

Table 39-1157 VirtualRouterDown

Alarm	Attributes	Applicable major release
Name: VirtualRouterDown (277) Type: configurationAlarm Package: vrrp.VirtualRouterDown Raised on class: vrrp.VrrpVirtualRouter	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualRouterDown	Release: • N/A
Description: The alarm is raised when the aggregated Operational State of a VR is Down.		
Raising condition: (('Aggregated Operational State' EQUAL 'Down'))		
Clearing condition: (('Aggregated Operational State' NOT EQUAL 'Down'))		
Remedial action: Check the configuration of both VRRP instances for the VRRP virtual router.		

Table 39-1158 VirtualServicesControllerDown

Alarm	Attributes	Applicable major release
Name: VirtualServicesControllerDown (8430) Type: virtualSwitchControllerAlarm Package: dctr.VirtualServicesControllerDown Raised on class: dctr.VirtualSwitchController	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ControllerNotOperationallyUp	Release: • N/A
Description: The alarm is raised when Virtual Services Controller is not operationally up.		
Raising condition: (('Operational State' EQUAL 'Down'))		
Clearing condition: (('Operational State' EQUAL 'Up'))		
Remedial action: This alarm can be cleared when virtual services controller is operationally up.		

Table 39-1159 VirtualSwitchDown

Alarm	Attributes	Applicable major release
Name: VirtualSwitchDown (4913) Type: virtualSwitchAlarm Package: dctr.VirtualSwitchDown Raised on class: dctr.AbstractVirtualSwitchGlobal	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ControllerDownOrPhysi-calPortDownOrInterfaceDown	Release: • N/A
Description: The alarm is raised when Openflow session to the virtual switch is lost.		
Remedial action: This alarm can be cleared when virtual switch is operationally up.		

Table 39-1160 VirtualSwitchIpAddressDuplicated

Alarm	Attributes	Applicable major release
Name: VirtualSwitchIpAddressDuplicated (5435) Type: virtualSwitchAlarm Package: dctr.VirtualSwitchIpAddressDuplicated Raised on class: dctr.AbstractVirtualSwitchGlobal	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: VirtualSwitchIpAddressMis-Configuration	Release: • N/A
Description: The alarm is raised when more than one virtual switches in the same domain have the same ip address. Virtual switches that are not belong or have not been associated to any domain are considered to be in 'undefined' domain.		
Remedial action: This might have caused by a network configuration. Please check the status of the Admin Domain and/or the Virtual Switch ip address and controller state. Please make sure the CPAA is managed, Admin Domain is operational, then unmanage the node with duplicate virtual switch ip address and remanage it again. This alarm must be cleared manually.		

Table 39-1161 VirtVpnBGPPrefixConflict

Alarm	Attributes	Applicable major release
Name: VirtVpnBGPPrefixConflict (5431) Type: virtualPortAlarm Package: dctr.VirtVpnBGPPrefixConflict Raised on class: dctr.AbstractVirtualPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateVswNextHop_ VmExistsOnTwoLocations	Release: • N/A
Description: The alarm is raised when routes or service context could be stuck in compute or the network.		
Remedial action: Routes or service context could be stuck in compute or the network. Reapply compute or network policies to reset the network attachment.		

Table 39-1162 VirtVpnBGPPrefixUnreachable

Alarm	Attributes	Applicable major release
Name: VirtVpnBGPPrefixUnreachable (5432) Type: virtualPortAlarm Package: dctr.VirtVpnBGPPrefixUnreachable Raised on class: dctr.AbstractVirtualPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VportCannotBeReachedFrom-BgpVpn	Release: • N/A
Description: The alarm is raised when there is no route for the VPN regardless of routing on the virtual port.		
Remedial action: There is no route for the VPN regardless of routing on the virtual port. This may be an RR/VSC policy issue or internal VSD policy issue; e.g. no route assigned.		

Table 39-1163 VirtVpnBGPPrefixUnstable (vpls)

Alarm	Attributes	Applicable major release
Name: VirtVpnBGPPrefixUnstable (9010) Type: serviceAlarm Package: vpls.VirtVpnBGPPrefixUnstable Raised on class: vpls.AbstractVpls	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: BgpNetworkUnstable	Release: • N/A
Description: The alarm is raised when BGP Prefix defined in Data Center BGP Profile has been matched and Alarm requested by user. The alarm is raised based on 1 min accumulation interval: if during this interval any appropriate BGP Prefix went unreachable OR flapped OR lost redundancy the alarm shall be raised.		
Remedial action: Navigate to DC Historical Correlation Events to see affected prefixes. Based on this info debug BGP Network		

Table 39-1164 VirtVpnBGPPrefixUnstable (vprn)

Alarm	Attributes	Applicable major release
Name: VirtVpnBGPPrefixUnstable (9010) Type: serviceAlarm Package: vprn.VirtVpnBGPPrefixUnstable Raised on class: vprn.Vprn	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: BgpNetworkUnstable	Release: • N/A
Description: The alarm is raised when BGP Prefix defined in Data Center BGP Profile has been matched and Alarm requested by user. The alarm is raised based on 1 min accumulation interval: if during this interval any appropriate BGP Prefix went unreachable OR flapped OR lost redundancy the alarm shall be raised.		
Remedial action: Navigate to DC Historical Correlation Events to see affected prefixes. Based on this info debug BGP Network		

Table 39-1165 VirtVpnBGPPrefixWithdrawnNotReceived

Alarm	Attributes	Applicable major release
Name: VirtVpnBGPPrefixWithdrawnNotReceived (5433) Type: virtualPortAlarm Package: dctr. VirtVpnBGPPrefixWithdrawnNotReceived Raised on class: dctr.AbstractVirtualPort	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VportAddressMismatchWithB-gpRoute	Release: • N/A
Description: The alarm is raised when there is no route on virtual port whereas BGP RIB has a route or routes which do not match.		
Remedial action: There is no route on virtual port whereas BGP RIB has a route or routes which do not match. Check compute and Nuage virtualization policies.		

Table 39-1166 VlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: VlanSubTypeConflict (227) Type: configurationAlarm Package: vlan.VlanSubTypeConflict Raised on class: vlan.Vlan	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • N/A
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a service.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN Subtype of the Site matches the VLAN Subtype of the Service.		

Table 39-1167 VLanUplinkDown

Alarm	Attributes	Applicable major release
Name: VLanUplinkDown (1146) Type: VLanUplinkAlarm Package: service.VLanUplinkDown Raised on class: service.VlanUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VLanUplinkDown	Release: • N/A
Description: The alarm is raised when a VLAN uplink is operationally down.		
Raising condition: (('Aggregation Operational State' EQUAL 'Partially Down') OR ('Aggregation Operational State' EQUAL 'Down'))		
Clearing condition: (('Aggregation Operational State' NOT EQUAL 'Partially Down') AND ('Aggregation Operational State' NOT EQUAL 'Down'))		
Remedial action: Check the underlying physical link for the SAPs.		

Table 39-1168 VLanUplinkNotCreated

Alarm	Attributes	Applicable major release
Name: VLanUplinkNotCreated (1147) Type: VLanUplinkAlarm Package: service.VLanUplinkNotCreated Raised on class: service.Service	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VLanUplinkNotCreated	Release: • N/A
Description: The alarm is raised when an expected VLAN uplink does not exist.		
Remedial action: Make sure the two participating ports which hold the uplink SAPs of the service are physically connected and operationally up. And make sure a physical link is created and is operationally up either by enabling LLDP or manually creating a physical link between those ports.If the physical link already exists and operationally up, make sure the uplink SAPs has been created with matching encapsulation values, in case the uplink SAPs has already been created with different encapsulation values, please delete those uplink SAPs and create the uplink SAPs with same encapsulation values.		

Table 39-1169 VNFCDown

Alarm	Attributes	Applicable major release
Name: VNFCDown (9583) Type: ConfigurationAlarm Package: nfv.VNFCDown Raised on class: nfv.VNFComponent	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: vmNotActive	Release: • N/A
Description: The alarm is raised when Virtual Network Function VM is not active.		
Remedial action: This alarm can be cleared when virtual network function resource is active.		

Table 39-1170 VnfResourceOperationFailed

Alarm	Attributes	Applicable major release
Name: VnfResourceOperationFailed (9612) Type: ConfigurationAlarm Package: nfv.VnfResourceOperationFailed Raised on class: nfv.VirtualNetworkFunction	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ResourceManagementAPI-CallToCloudManagerFail	Release: • N/A
Description: The alarm is raised when Virtual Network Function resource is not operationally up.		
Remedial action: User can check for the statusReason to find the cause of failure and retry. This alarm can be cleared when virtual network function request is successful.		

Table 39-1171 VoiceChannelLoopback

Alarm	Attributes	Applicable major release
Name: VoiceChannelLoopback (1148) Type: configurationAlarm Package: tdmequipment.VoiceChannelLoopback Raised on class: tdmequipment.VoiceChannelSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: voiceChannelLoopback	Release: • N/A
Description: The alarm is raised when an NE reports that a voice channel has a loopback alarm condition.		
Remedial action: Informational only.		

Table 39-1172 vPortHostMatchFailure

Alarm	Attributes	Applicable major release
Name: vPortHostMatchFailure (3628) Type: configurationAlarm Package: equipment.vPortHostMatchFailure Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tPortEgrVPortHostMatchFail-ure	Release: • N/A

Table 39-1172 vPortHostMatchFailure (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a host match lookup fails to resolve the egress virtual port.		
Remedial action: This alarm is raised when the subscriber host with an intermediate destination ID that does not match the host-match destination set under the V-port. \nModify the intermediate destination ID of the subscriber host to match the host-match defined in the v-port; Or modify the host-match destination ID to match the intermediate destination ID of the subscriber host.		

Table 39-1173 VprnTypeMismatched

Alarm	Attributes	Applicable major release
Name: VprnTypeMismatched (8149) Type: configurationAlarm Package: vprn.VprnTypeMismatched Raised on class: vprn.Vprn	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: vprnTypeMismatched	Release: • N/A
Description: The alarm is raised when the newly created VPRN Site has a VPRN type that is of a different topology from existing VPRN Sites of the service, i.e, mesh vs hub/spoke, or vice versa.		
Remedial action: A configuration error has occurred which should be corrected. The VPRN type of the created site is of a different topology type from the existing VPRN Sites of the service, i.e., mesh and hub/spoke sites shall not be mixed in the same service. The service shall be deleted and re-created with consistent type.		

Table 39-1174 VSiteServiceImpacted

Alarm	Attributes	Applicable major release
Name: VSiteServiceImpacted (5430) Type: serviceAlarm Package: dctr.VSiteServiceImpacted Raised on class: dctr.AbstractVirtualSite	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualPortReachability	Release: • N/A
Description: The alarm is raised on the VSite object when there is an alarm on VPort that affects service.		
Remedial action: One or more virtual ports are down or have BGP reachability problem such as stuck or unreachable prefix. This alarm can be cleared when the corresponding alarms on virtual ports are cleared.		

Table 39-1175 VwmShelfCardRemoved

Alarm	Attributes	Applicable major release
Name: VwmShelfCardRemoved (5661) Type: equipmentAlarm Package: equipment.VwmShelfCardRemoved Raised on class: equipment.VWMCardSlot	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfCardRemoved	Release: • N/A
Description: The alarm is raised when a vwm card is removed.		
Remedial action: Informational - a vwm shelf card has been removed from the NE		

Table 39-1176 VwmShelfMismatch

Alarm	Attributes	Applicable major release
Name: VwmShelfMismatch (4941) Type: equipmentAlarm Package: equipment.VwmShelfMismatch Raised on class: equipment.VwmShelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfMismatch	Release: • N/A
Description: The alarm is raised when the configured vwm shelf id is different than the equipped vwm shelf.		
Remedial action: This alarm is raised when the detected VWM shelf id does not match the provisioned id. Please follow the below steps to clear this alarm:\n a. Check the id on the rotary dial on the VWM SHelf.\n b. Use any of the following commands to clear the alarm. \n c. To change the VWM shelf id("config system vwm-shelf <shelf-id> .\n d. To delete an existing shelf("config system no vwm-shelf <shelf-id>").		

Table 39-1177 VwmShelfRemoved

Alarm	Attributes	Applicable major release
Name: VwmShelfRemoved (4942) Type: equipmentAlarm Package: equipment.VwmShelfRemoved Raised on class: equipment.VwmShelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VwmShelfRemoved	Release: • N/A
Description: The alarm is raised when a vwm shelf is removed.		
Remedial action: Informational - a vwm shelf has been removed from the NE		

Table 39-1178 WaitToRevertMismatchAlarm

Alarm	Attributes	Applicable major release
Name: WaitToRevertMismatchAlarm (8425) Type: integrityViolation Package: gmpls.WaitToRevertMismatchAlarm Raised on class: gmpls.DbLink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: waitToRevertMismatch	Release: • N/A
Description: The alarm is raised when the Wait to Revert (WTR) configured on the endpoints of the DB Link do not match.		
Remedial action: This alarm indicates that the Wait to Revert (WTR) configured on the endpoints of the discovered DB Link do not match. Please make sure the WTR is the same on the databearers at each end.		

Table 39-1179 WmmLSS_nodeGroupOOS

Alarm	Attributes	Applicable major release
Name: WmmLSS_nodeGroupOOS (4808) Type: mmeAlarm Package: ltemme.WmmLSS_nodeGroupOOS Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • N/A

Table 39-1179 WmmLSS_nodeGroupOOS (continued)

Alarm	Attributes	Applicable major release
Description: This Major alarm occurs when a Node Group state enters Redundancy. This Critical alarm occurs when a Node Group state enters Fault.		
Remedial action: The alarm is cleared when the node group state changed to Normal, i.e. all the nodes in this node group enter In Service(unblocked) state.\nDetermine that there are no errors within the IP network. If errors exist, follow the operating procedures to correct these errors.\nDetermine that the Ethernet Switch Card (ESC) is in service. If not, follow the local operating procedures to restore the ESC to service.\nDetermine that the DNS is provisioned with correct IP addresses for the Destination URI. If not, correctly provision the DNS with the correct IP addresses for the Destination URI.		

Table 39-1180 WmmLSS_nodeOOS

Alarm	Attributes	Applicable major release
Name: WmmLSS_nodeOOS (4809) Type: mmeAlarm Package: ltemme.WmmLSS_nodeOOS Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • N/A
Description: This alarm indicates the state of a Node has changed from in-service to out-of-service.		
Remedial action: Determine if the destination URI is in service and is able to respond to the SIP heartbeat. If not, follow the operating procedures to restore the destination URI to service.\nDetermine that there are no errors within the IP network. If errors exist, follow the operating procedures to correct these errors.\nDetermine that the Ethernet Switch Card (ESC) is in service. If not, follow the local operating procedures to restore the ESC to service.\nDetermine that the DNS is provisioned with correct IP addresses for the Destination URI. If not, correctly provision the DNS with the correct IP addresses for the Destination URI.		

Table 39-1181 WmmLSS_rccInhibitedMode

Alarm	Attributes	Applicable major release
Name: WmmLSS_rccInhibitedMode (4810) Type: mmeAlarm Package: ltemme.WmmLSS_rccInhibitedMode Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • N/A
Description: This alarm will be raised when RCC is set to inhibited mode on a host. Inhibited mode will prevent any service on that host from being switched over to its mate, or from failing over to its mate, and is typically used only during maintenance activities such as software upgrade or patching.		
Remedial action: The alarm will clear automatically when the RCC inhibit flag is cleared on the affected host.\n1. To display the RCC inhibit flag on a host, run this command on the MI: For ATCA: rcc_adm --action disp_inhibit --host <amp value="'lt'/>hostname<amp value='gt'/> For cPSB: rccInhibit -d <amp value='lt'/>hostname<amp value='gt'/> where <amp value='lt'/>hostname<amp value='gt'/> is the affected host name\n2. To clear the RCC inhibit flag on a host, run this command from the MI: For ATCA: rcc_adm --action clr_inhibit --host <amp value='lt'/>hostname<amp value='gt'/> For cPSB: rccInhibit -a CLEAR <amp value='lt'/>hostname<amp value='gt'/> where <amp value='lt'/>hostname<amp value='gt'/> is the affected host name\nIf the alarm does not clear after clearing the RCC inhibit flag, contact your Nokia support representative"		

Table 39-1182 WmmLSS_sipLinkSetMaxQuarantineList

Alarm	Attributes	Applicable major release
Name: WmmLSS_sipLinkSetMaxQuarantineList (4811) Type: mmeAlarm Package: ltemme.WmmLSS_sipLinkSetMaxQuarantineList Raised on class: ltemme.MmeAlarmEntry	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: mmeUnspecifiedReason	Release: • N/A
Description: This alarm occurs when the maximum number of out of service SIP linkset has been reached in the quarantine list.		
Remedial action: need manual procedure to clear the alarm		

Table 39-1183 WMMSoftwareUpgradeInProgress

Alarm	Attributes	Applicable major release
Name: WMMSoftwareUpgradeInProgress (9603) Type: configurationAlarm Package: sw.WMMSoftwareUpgradeInProgress Raised on class: sw.SoftwareUpgradeManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: softwareUpgradeInProgress	Release: • N/A
Description: This alarm is raised when SAM detects that a WWM Software Upgrade status is 'in-progress' on server start-up.		
Remedial action: SAM has detected that the WMM Software Upgrade status is 'in-progress' on server start-up. Run a Software Inventory to correctly update the status or Continue if 'Image Files Transfer Failed'. You may have to wait until the operation finishes executing on the node in order to get into a 'Continue' state.		

Table 39-1184 WriteFileToDisk

Alarm	Attributes	Applicable major release
Name: WriteFileToDisk (1940) Type: serverAlarm Package: server.WriteFileToDisk Raised on class: server.SamServer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: false Default probable cause: diskSpaceIssue	Release: • N/A
Description: The alarm is raised when SAM cannot write a file to disk.		
Remedial action: Check the additional text of the alarm for more details. Possible causes are lack of disk space or insufficient file permissions. The additional text will provide guidance as to the specifics of the problem.		

Table 39-1185 XPICCableLoss

Alarm	Attributes	Applicable major release
Name: XPICCableLoss (4851) Type: communicationsAlarm Package: mwa.XPICCableLoss Raised on class: mwa.PortTermination	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DemodulatorXPICLossOfSignal	Release: • N/A
Description: The alarm is raised when a MPT detects a XPIC plug-in cable loss		
Remedial action: Please refer to either 9500 or 7705 Node Maintenance manual for remedial action information.		

Table 39-1186 XpIIngrError

Alarm	Attributes	Applicable major release
Name: XpIIngrError (8382) Type: hardwareAnomaly Package: equipment.XpIIngrError Raised on class: equipment.DaughterCard	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: XpIIngrError	Release: • N/A
Description: The alarm is raised when an MDA reports persistent Ingress XPL Errors.		
Remedial action: Informational - if the condition persists then the MDA indicated in the alarm should be replaced.		

Table 39-1187 YellowAlarmThresholdReached

Alarm	Attributes	Applicable major release
Name: YellowAlarmThresholdReached (245) Type: communicationsAlarm Package: netw.YellowAlarmThresholdReached Raised on class: netw.NmsSystem	Severity: critical Specific problem: Not Applicable Implicitly cleared: false Default probable cause: tooManyAlarms	Release: • N/A
Description: The alarm is raised when the number of outstanding 5620 SAM alarms reaches the yellow threshold. When this happens, the 5620 SAM discards non-critical alarms to keep the number below the threshold.		
Remedial action: Informational - if the alarm persists or is occurring frequently perform root cause analysis to determine why the NEs in the network are consistently generating high rates of alarms.		

40 Nokia - FDD Airscale

40.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 40-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • FL16A
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 40-2 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • FL16A
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 40-3 AUTO_NEGO_MIS_MATCH

Alarm	Attributes	Applicable major release
Name: AUTO_NEGO_MIS_MATCH (11513) Type: communicationsAlarm Package: racfl.AUTO_NEGO_MIS_MATCH Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: AUTO NEGO MIS MATCH Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: AUTO NEGO MIS MATCH\n\nThis alarm indicates that there is a mismatch between the BTS configuration and the auto-negotiation result.\n\nIf the alarm is active, a synchronization loop is possible.\n\n		
Remedial action: Flexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nTry with local management or site support equipment.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone:\nConfirm that the Ethernet Synchronization master/slave settings are correct on the Flexi Zone Micro BTS or Flexi Zone Access Point and backhaul equipment. \nNote: The Flexi Zone Micro BTS and Flexi Zone Access Point only support slave mode.		

Table 40-4 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • FL16A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 40-5 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • FL16A
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 40-6 BASE_STATION_CONNECTIVITY_DEGRADED

Alarm	Attributes	Applicable major release
Name: BASE_STATION_CONNECTIVITY_ DEGRADED (11514) Type: communicationsAlarm Package: racfl.BASE_STATION_CONNECTIVITY_ DEGRADED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION CONNECTIVITY DEGRADED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION CONNECTIVITY DEGRADED\n\nA major fault (or faults) has occured in the base station interface. Check the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-6 BASE_STATION_CONNECTIVITY_DEGRADED (continued)

Alarm	Attributes	Applicable major release
Remedial action: FAULT NAME\nGTP-U Path Failure\n\nFAULT ID\n6150: EFaultId_GtpuPathFailure\n\nMEANING\nIn GTP-U supervision, a network element did not respond to the GTP-U: Echo Request message within the allotted time.\n\nINSTRUCTIONS\n1. Check the GTP-U path supervision configuration of the eNB. \n2. Check if the supervised network element is operating correctly.\n3. Check the communication equipment between the eNB and the supervised network element.\n\nIn case actDualUPlaneIpAddress =" true, the S-GW might still be reachable although an alarm caused by fault 6150 is reported.\nCheck whether other alarms caused by fault 6150 are active, and check whether all GTP-U paths to the S-GW are concerned or not. If you find that all GTP-U paths to the same S-GW are faulty, the S-GW is not reachable anymore.\n\n\n\n\nFAULT NAME\nM3 interface recovery failure\n\nFAULT ID\n6850: EFaultId_M3ResetRetryOut\n\nMEANING\nM3 interface reset has failed after several attempts. This indicates that a severe failure has occurred. There might be some configuration problem, there is no M3 connectivity, MME has failed, and so on.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears.\n\n1. Check the availability of MME.\n2. Check the connection with MME.\n3. Disconnect and reconnect MME.\n\n\n\n\nFAULT NAME\nM3 interface setup failure\n\nFAULT ID\n6851: EFaultId_M3SetupFailure\n\nMEANING\nThere is no M3 connectivity to an MME, the MME has failed, and so on. If the fault is canceled, autonomous recovery actions (reset) have solved the fault situation.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check availability of MME.\n2. Check other faults on MME and BTS.\n3. Check the parameters related to M3 interface in the BTS and MME.\n4. Reset the BTS.\n\n\n\n\nFAULT NAME\nRIM interface error\n\nFAULT ID\n6323: EFaultId_RimInterfaceError\n\nMEANING\n1. An RIM association could not be established because an RIM Error PDU has been received for an RIM-enabled GERAN neighbor cell.\n2. An RIM Application Error has been detected.\n3. S1 links to all configured MMEs are active, but the routing of RIM PDU to the RIM-enabled WCDMA neighbor cell is not available.\n\nINSTRUCTIONS\nCheck the value of the parameter "rimStatus" in LNADJG or LNADJW (according to the alarm source) objects to find all impacted RIM associations.\n\nIf only a few LNADJG or LNADJW objects have "rimStatus" Unavailable, check if LNADJG or LNADJW identifiers (cell global ID) of related GERAN or UTRAN cells are correct.\n\nIf many LNADJG or LNADJW objects have "rimStatus" Unavailable, check the connectivity to GSM or WCDMA network (MME<->SGSN<->BSC).\n\nNote that only one alarm for one PLMN is raised due to the RIM faults for GERAN and only one for UTRAN, no matter how many LNADJGs or LNADJWs are affected at a given time. The alarm is raised for the first LNAJDG or LNADJW where the fault is detected. The alarm additional information contains the parameters of the first LNADJG or LNADJW, even if the RIM fault is already inactive for the LNADJG or LNADJW, but the fault is still active for other LNADJG or LNADJW supporting the same PLMN.\n\n\n\n\nFAULT NAME\nRIM interface timeout\n\nFAULT ID\n6322: EFaultId_ RimInterfaceTimeout\n\nMEANING\nA RIM request to the serving BSS has failed after several attempts. This means that the System Information for the related GERAN or UTRAN neighbor cells is not reliable.\n\nINSTRUCTIONS\nCheck the value of the parameter "rimStatus" in LNADJG or LNADJW (according to the alarm source) objects to find all impacted RIM associations.\n\nIf only a few LNADJG or LNADJW objects have "rimStatus" Unavailable, check if the LNADJG or LNADJW identifiers (cell global ID) of the related GERAN or UTRAN cells are correct.\n\nIf many LNADJG or LNADJW objects have "rimStatus" Unavailable, check the connectivity to the GSM or WCDMA network (MME<->SGSN<->BSC).\n\nNote that only one alarm for one PLMN is raised due to the RIM faults for GERAN, and only one for UTRAN no matter how many LNADJGs or LNADJWs are affected at a given time. The alarm is raised for the first LNAJDG or LNADJW where the fault is detected. The alarm additional information contains the parameters of the first LNADJG or LNADJW even if the RIM fault is already inactive for the LNADJG or LNADJW, but the fault is still active for other LNADJG or LNADJW supporting the same PLMN.\n\n\n\n\nFAULT NAME\nS1 interface recovery failure\n\nFAULT ID\n6317: EFaultId_S1ResetRetryOut\n\nMEANING\nThe S1 interface reset has failed after several attempts. This indicates that a severe failure has occurred: there is some configuration problem; there is no S1 connectivity; MME has failed; and so on.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check the availability of the MME.\n2. Check the connection with the MME.\n3. Disconnect and reconnect the MME.\n\n\n\n\nFAULT NAME\nS1 interface setup failure\n\nFAULT ID\n6308: EFaultId_ S1SetupRetryOut\n\nMEANING\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nThere is no S1 connectivity to an MME. \n\nThe fault is generated if the S1 setup procedure has subsequently been attempted but failed the number of times equal to "maxS1SetRetry".\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nThere is no S1 connectivity to an MME, the MME has failed, and so on. If the fault is cancelled, autonomous recovery actions (reset) will solve the fault situation.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check the availability of the MME.\n2. Check other faults on the MME and BTS.\n3. Check the parameters related to the S1 interface in the BTS and MME.\n4. Reset the BTS.\n\n\n\n\nFAULT NAME\nS1 SCTP path failure\n\nFAULT ID\n6204: EFaultId_S1SctpPathAl\n\nMEANING\nOne of the transport paths (SCTP) in SCTP connection to the MME has failed. This is only applicable when SCTP multi-homing is supported. An alternate transport path is available to continue operation.\n\nINSTRUCTIONS\n1. Check whether the transport path is alive.\2. Check the configuration of transport addresses at MME.\n\n\n\n\nFAULT NAME\nToggling: <Fault name>\n\nFAULT ID\n4026: EFaultId_TogglingAl\n\nMEANING\nThis alarm is used to inform the operator that another BTS fault (the original fault) is toggling.\nThe alarm that is related to the original fault is suppressed and the new alarm, which is related to fault 4026: EFaultId_TogglingAlFault, is raised.\n\nToggling alarms that are related to the original faults are suppressed until the toggling condition is cleared.\n\nThe severity of this BTS fault is the same as the severity of the original\ntoggling BTS fault.\n\nINSTRUCTIONS\n1. Check the fault name of the toggling BTS fault. \n2. Follow the instructions of the toggling BTS fault to clear the problem.\n \nNote: Detailed information about the toggling frequency can be found in the alarm history file, which can be downloaded using BTS Site Manager. The log file is available with Snapshot.\n\n\n\n\nFAULT NAME\nTransport layer connection failure in M3 interface\n\nFAULT ID\n6205: EFaultId_M3SctpEndpointAl\n\nMEANING\nThe transport path (SCTP) for connection to MME has been broken. The reason for this can be an unplugged cable to MME. No transport path is available to pursue operation on the faulty connection with the MME.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n1. Check the connection with MME, particularly whether the M3 link is broken.\n2. Check if the MME is operational.\n3. Check if the speed and duplex setting of eNB M3 port is consistent with switch port, which is connected directly to the eNB for example both "Autodetect" or both "1000 Mbit/s Full duplex".\n\nIf this fault happens right after a commissioning or a configuration change, verify the following configuration data: IP address of the MME.\n\n\n\n\nFAULT NAME\nTransport layer connection failure in S1 interface\n\nFAULT ID\n6202: EFaultId_S1SctpEndpointAl\n\nMEANING\nThe transport path (SCTP) for connection to the MME is broken. This might be because of an unplugged cable to the MME. There is no transport path available to continue operation on the faulty connection with the MME.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1.		

Table 40-7 BASE_STATION_CONNECTIVITY_LOST

Alarm	Attributes	Applicable major release
Name: BASE_STATION_CONNECTIVITY_LOST (11515) Type: communicationsAlarm Package: racfl.BASE_STATION_CONNECTIVITY_LOST Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION CONNECTIVITY LOST Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION CONNECTIVITY LOST\n\nA critical fault (or faults) has occured in the base station interface.\nCheck the reason for the fault from the supplementary text field of the\nalarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when\nthe fault has been corrected.		
Remedial action: FAULT NAME\nS1 interface recovery failure\n\nFAULT ID\n6317: EFaultId_S1ResetRetryOut\n\nMEANING\nThe S1 interface reset has failed after several attempts. This indicates that a severe failure has occurred: there is some configuration problem; there is no S1 connectivity; MME has failed; and so on.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check the availability of the MME.\n2. Check the connection with the MME.\n3. Disconnect and reconnect the MME.\n\n\n\n\nFAULT NAME\nS1 interface setup failure\n\nFAULT ID\n6308: EFaultId_S1SetupRetryOut\n\nMEANING\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nThere is no S1 connectivity to an MME. \n\nThe fault is generated if the S1 setup procedure has subsequently been attempted but failed the number of times equal to "maxS1SetRetry".\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nThere is no S1 connectivity to an MME, the MME has failed, and so on. If the fault is cancelled, autonomous recovery actions (reset) will solve the fault situation.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check the availability of the MME.\n2. Check other faults on the MME and BTS.\n3. Check the parameters related to the S1 interface in the BTS and MME.\n4. Reset the BTS.\n\n\n\n\nFAULT NAME\nToggling: <Fault name>\n\nFAULT ID\n4026: EFaultId_TogglingAl\n\nMEANING\nThis alarm is used to inform the operator that another BTS fault (the original fault) is toggling.\nThe alarm that is related to the original fault is suppressed and the new alarm, which is related to fault 4026: EFaultId_TogglingAlFault, is raised.\n\nToggling alarms that are related to the original faults are suppressed until the toggling condition is cleared.\n\nThe severity of this BTS fault is the same as the severity of the original\ntoggling BTS fault.\n\nINSTRUCTIONS\n1. Check the fault name of the toggling BTS fault. \n2. Follow the instructions of the toggling BTS fault to clear the problem.\n \nNote: Detailed information about the toggling frequency can be found in the alarm history file, which can be downloaded using BTS Site Manager. The log file is available with Snapshot.\n\n\n\n\nFAULT NAME\nTransport layer connection failure in S1 interface\n\nFAULT ID\n6202: EFaultId_S1SctpEndpointAl\n\nMEANING\nThe transport path (SCTP) for connection to the MME is broken. This might be because of an unplugged cable to the MME. There is no transport path available to continue operation on the faulty connection with the MME.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears:\n\n1. Check the connection with the MME, accordingly, based on whether the S1 link is broken.\n2. Check if the MME is operational.\n3. Check if the speed and duplex setting of the eNB S1 port is consistent with the switch port that is connected directly to the eNB (for example, they are both "Autodetect" or both "1000 Mbit/s Full duplex").\n\nIf this fault happens right after a commissioning or a configuration change, verify the IP address of the MME.		

Table 40-8 BASE_STATION_FAULTY

Alarm	Attributes	Applicable major release
Name: BASE_STATION_FAULTY (11516) Type: equipmentAlarm Package: racfl.BASE_STATION_FAULTY Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION FAULTY Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION FAULTY\n\nA critical fault (or faults) has occurred in the base station.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-8 BASE_STATION_FAULTY (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see the source of the alarm and instructions fields of the corresponding alarms). \n\nIn case of the FSM failure (FSM or FSM sub-unit is reported as source) it is possible that other units are also reported as faulty since it is impossible for them to continue functioning without a system module. In such case replace the system module first and check if the modules previously marked as Faulty are now in Working state.\n\n\nBelow is the list of BTS fault(s) which may have caused this alarm in BTS FL16A/TL16A release. In the case of an earlier SW release and if you need more detailed fault descriptions, LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n\nFAULT NAME\nAntenna link is down\n\nFAULT ID\n476: EFaultId_Rp3BusError\n\nMEANING\nThe antenna (RP3) link is down. The transmitter or receiver drops from synchronization.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Restart the BTS.\n2. If that does not help, replace the alarming module. \n\nFlexi BTS FDD/TDD: In case the FSP is causing the alarm, replace the FSM because the alarm is related to the fixed FSP inside the FSM. \n\nFlexi BTS FDD/TDD, AirScale BTS FDD/TDD: If FBBx or ABIx is causing the alarm, replace the FBBx or ABIx.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone, Flexi Zone SFN Antenna: Replace the Flexi Zone Micro BTS, Flexi Zone Access Point, or Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nAP blocked\n\nFAULT ID\n4260: EFaultId_ApBlockedAl\n\nMEANING\nThe Flexi Zone Access Point is blocked by the BTS Site Manager. This is done to avoid fault indications that might be raised during a Flexi Zone Access Point maintenance task.\n\nINSTRUCTIONS\nTo cancel the fault, unblock the Flexi Zone Access Point.\n\n\n\n\nFAULT NAME\nBaseband bus configuration of <x> was rejected\n\nFAULT ID\n1811: EFaultId_BbBus_ConfFailedAl\n\nMEANING\nThe baseband-bus-related configuration of <x> has been rejected by the HW SW, DSP, or RF SW.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nReplace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Download the correct configuration.\n2. Reset the BTS.\n3. Replace the BTS.\n\nFlexi Zone:\n1. Download the correct configuration.\n2. Reset the Flexi Zone Access Point from the BTSSM.\n3. Replace the Flexi Zone Access Point.\n\nFlexi Zone SFN Antenna:\n1. Download the correct configuration.\n2. Reset the Flexi Zone SFN Antenna from the BTSSM.\n3. Replace the Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nBaseband bus failure\n\nFAULT ID\n3020: EFaultId_BaseBandBusFailure\n\nMEANING\nThe Flexi BTS has detected an abnormal operation or a failure in the BTS\ninternal or external (optical link) baseband bus. The failure cannot be\nattributed to a specific module and there are several possible fault sources.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the other active BTS faults and act accordingly.\n\n2. Check the cables between the System Module and RF Module.\n\n3. Reset the RF Module and/or System Module, depending on the alarm source:\n a. Reset the RF Module by blocking and unblocking it.\n b. Reset the System Module by blocking and unblocking it.\n\n4. Replace the alarming RF Module.\n\n5. If the System Module is the source, or replacing the RF Module does not clear the fault situation, replace the alarming System Module.\n\n\n\n\nFAULT NAME\nBaseband resources mapping to cells failure\n\nFAULT ID\n12: EFaultId_TcomConfigAl\n\nMEANING\nA failure is detected when the eNodeB O&M system presents available FSPs to C-plane software in order to map FSPs to a cell. The FSPs related to the faulty operation cannot be taken into use. The reason for the failure might be an internal problem in the eNodeB O&M system.\n\nINSTRUCTIONS\n1. Block and unblock the BTS.\n2. Perform a power-off reset. \n3. If steps 1 and 2 do not help, replace the module that is causing the\nalarm. \n\n\n\n\nFAULT NAME\nBB bus reception error (summing device)\n\nFAULT ID\n2016: EFaultId_Muksu_SMTimeOffAl\n\nMEANING\nThe master frame in the received baseband bus frame is not in the correct place related to the internally-generated master frame pulse. Either the frame has been set into the wrong place (PI delay), or the data itself is in the wrong place.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module, the cable between the FBBx/ABIx module and the RF module, and the cable between the system module and the FBBx module.\n\n2. Replace the unit that causes the alarm (system module or FBBx/ABIx).\n\n\n\n\nFAULT NAME\nBB bus transmission error\n\nFAULT ID\n2017: EFaultId_Muksu_SRx10b8bAl\n\nMEANING\nA decoding error has been detected in the baseband internal link. The data packet is lost, or the content is corrupted.\n\nThis situation also occurs when the links are not synchronized with each other.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module, and the cable between the FBBx/ABIA module and the RF module.\n\n2. Reset the system module.\n\n3. Replace the alarming module (system module).\n\n\n\n\nFAULT NAME\nBoot configuration inconsistency detected\n\nFAULT ID\n4102: EFaultId_BootConfigurationInconsistencyAl\n\nMEANING\nDuring SW update, the configurations of the active and passive SW in the HW unit have been detected to be the same. Active and passive SW configurations are compared at these periods:\n- before SW download\n- during SW activation, before active and passive SW switch\n- during start-up\n\nINSTRUCTIONS\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Block/unblock the Flexi Zone Micro BTS to reset.\n2. If blocking or unblocking the Flexi Zone Micro BTS does not solve the problem, replace the faulty Flexi Zone Micro BTS.\n\nFlexi Zone Access Point, Flexi Zone SFN Antenna:\nNone\n\n\n\n\nFAULT NAME\nBTS blocked\n\nFAULT ID\n50: EFaultId_BTSBlockedAl\n\nMEANING\nThe BTS is blocked with the BTS Site Manager. The purpose is to avoid fault indications that might be raised during a BTS maintenance task.\n\nINSTRUCTIONS\nUnblock the BTS to cancel the fault. Unblocking the BTS causes a BTS reset.\n\n\n\n\nFAULT NAME\nBTS file error\n\nFAULT ID\n1802: EFaultId_FileRequestFlashAl\n\nMEANING\nA software download to FSP, DSP, ABIx or FR has failed.\n\nINSTRUCTIONS\nNote: Perform the following steps in the listed order until the fault disappears:\n\n1. Use BTS Site Manager to perform a full commissioning to the BTS using the NetAct backup upload SCF file as template.\n\n2. Download two different software packages so that the faulty file is removed from the BTS.\n\n3. Download the software again.\n\n4. Replace the System Module.\n\n\n\n\nFAULT NAME\nBTS internal SW management problem\n\nFAULT ID\n3090: EFaultId_BtsInternalSwManagementProblem\n\nMEANING\nA software update to a module or sub-assembly has failed, or a corrupted SW file has been detected in the FLASH.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears:\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Check the other active BTS faults. If the ROM disk is corrupted, change the alarming module.\n2. Reset the RF Module and/or System Module (depending on the fault source) by blocking/unblocking it.\n3. Update and activate the SW to the BTS.\n4. Check the SW files.\n5. Replace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Check the other active Flexi Zone Micro BTS or Flexi Zone Access Point faults. If the ROM disk is corrupted, change the Flexi Zone Micro BTS or Flexi Zone Access Point.\n2. Reset the Flexi Zone Micro BTS		

Table 40-9 BASE_STATION_LICENSE_LIMITATION

Alarm	Attributes	Applicable major release
Name: BASE_STATION_LICENSE_LIMITATION (11517) Type: qualityOfServiceAlarm Package: racfl.BASE_STATION_LICENSE_LIMITATION Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION LICENSE LIMITATION Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION LICENSE LIMITATION\n\nA critical fault (or faults) has occurred in the base station connectivity/interface. Check the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on\nthe fault description. For more information, see base station fault descriptions\nin LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: FAULT NAME\nActive users license limitation\n\nFAULT ID\n4337: EFaultId_ActiveUsersLimitAl \n\nMEANING\nThe eNB enters capacity limited mode due to missing licenses. Calls from excess users will be rejected except for handover and emergency calls.\n\nINSTRUCTIONS\nAdd licenses to the Centralized License Server to avoid call limitation.\nSee "Centralized License Server Help" document in NOLS for details.\n\n\n\n\n\nFAULT NAME\nCell Shutdown Due To Baseband Capacity License Limit\n\nFAULT ID\n4349: EFaultId_CellShutdownDueToBasebandCapacityLicenseLimitAl\n\nMEANING\nThe cell is shut down because it occupies baseband capacity that is over the licensed limit.\n\n\nINSTRUCTIONS\nAdd licenses to the Centralized License Server to avoid the traffic limitation.\nSee "Centralized License Server Help" document in NOLS for details.\n\n\n\n\n\nFAULT NAME\nIP Traffic Capacity Limit\n\nFAULT ID\n4293: EFaultId_IPTrafficCapacityLimitAl\n\nMEANING\nThe user's eNB IP traffic is throttled because of a missing license.\n\nINSTRUCTIONS\nRead the alarm diagnostic information to know when the missing license was detected and at what level the IP traffic is currently throttled in relation to the peak rate.\n\nAdd licenses to CLS to avoid the traffic limitation.\n\nIf licenses are not added, the level will be decreased to the lowest level, which is 50% of peak rate.		

Table 40-10 BASE_STATION_NOTIFICATION

Alarm	Attributes	Applicable major release
Name: BASE_STATION_NOTIFICATION (11518) Type: equipmentAlarm Package: racfl.BASE_STATION_NOTIFICATION Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION NOTIFICATION Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION NOTIFICATION\n\nA minor fault (or faults) has occurred in the base station.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-10 BASE_STATION_NOTIFICATION (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see source of the alarm and instructions fields of the corresponding alarms). \n\nBelow is the list of BTS faults which might have caused this alarm in BTS FL16A/TL16A release. In case of earlier SW release and in case you need more detailed fault descriptions refer to LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n\n----------\nFAULT NAME\n# autonomous reset as recovery action\n\nFAULT ID\n52: EFaultId_UnitAutonomousResetAl\n\nMEANING\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nThe fault informs the operator that the BTS is trying to correct a fault situation by performing a recovery reset to a unit, the site, or the BTS. \nIn case of an RF module reset in RF chaining configuration, the BTS also resets all RF modules that are further in the chain.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone, Flexi Zone SFN Antenna:\nThe BTS tries to recover from a fault situation by performing a site reset.\n\nINSTRUCTIONS\nCheck the fault history and other active faults of the unit.\n\nNote: This fault does not require any (special) actions.\n\n\n\n\nFAULT NAME\n10b8b coding error in optical interface device\n\nFAULT ID\n2004: EFaultId_OIC_LVDSRecAl\n\nMEANING\nThe fiber cable is experiencing interference; data transmission is faulty.\n\nA physical connection failure between the optical interface and the summing function has occurred.\n\nThe reason of the fault might be a low-quality or polluted SFP, or a low-quality optical cable used to connect radio module to system module/extension baseband module.\n\n\nINSTRUCTIONS\nNote: Perform the steps in the listed order until the fault is resolved.\n\n1. Reset the radio module behind the cable reported as the fault source by blocking/unblocking it. \n2. Reset the system module. \n3. Replace the SFP on the radio module port where the cable reported as fault source is terminated.\n4. Replace the SFP on the system module or extension baseband module port where the cable reported as fault source is terminated.\n5. Replace the optical cable reported as fault source.\n6. Replace the radio module behind the cable reported as fault source.\n7. If the system module reset helped but the fault is reported again after some time or if the actions mentioned above have not cleared the fault situation, replace the extension baseband module (if the fault is reported on the cable connected to the baseband module) or the system module (if the fault is reported on the cable connected to the system module).\n\n\n\n\nFAULT NAME\n2M external reference missing\n\nFAULT ID\n1899: EFaultId_2MExtRefMissAl\n\nMEANING\nThe reference clock monitoring has detected a signal loss of 2.048 MHz received from an external reference source, connected to Sync In interface of the System Module.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears.\n\n1. Check the cabling (connected to Sync In interface).\n\n2. Check if the 2.048 MHz reference source is working normally, and the 2.048 MHz signal is available.\n\n3. Replace the alarming module.\n\n\n\n\nFAULT NAME\n3GPP/AISG communication administratively disabled\n\nFAULT ID\n4142: EFaultId_Communication3gppAdministrativelyDisabledAl\n\nMEANING\nThe HDLC link has been disabled for the reporting Antenna Line or IUANT port.\n\nINSTRUCTIONS\nEnable the parameter "Communication3gppEnabled" for the reporting Antenna Line to revert changes.\n\n\n\n\nFAULT NAME\nAbnormal CPRI interface to next hop <OptIf ID>\n\nFAULT ID\n1974: EFaultId_AbnormalCpriInterfaceToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThe CPRI transmission is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The Optif is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is causing the alarm (connected to the faulty optical link, to the end farther from the system module).\n\n\n\n\nFAULT NAME\nAbnormal CPRI interface to upper hop <OptIf ID>\n\nFAULT ID\n1965: EFaultId_AbnormalCpriInterfaceToUpperHopAl\n\nMEANING\nThe optical interface does not work properly. CPRI transmission to the upper hop does not work properly.\n\nINSTRUCTIONS\nExecute the following steps in the ordered sequence. If any of the step does not help, execute the next one:\n\n1. Reset the radio module behind the cable reported as the fault source. \n2. Reset the system module. \n3. Replace the SFP on the radio module port where the cable reported as the fault source is terminated.\n4. Replace the SFP on the system module or the extension baseband module port where the cable reported as the fault source is terminated.\n5. Replace the optical cable reported as the fault source.\n6. Replace the radio module behind the cable reported as the fault source.\n7. If the actions mentioned above did not clear the faulty situation, replace the extension baseband module (if the fault is reported on the cable connected to the baseband module) or the system module (if the fault is reported on the cable connected to the system module).\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to next hop <OptIf ID>\n\nFAULT ID\n1973: EFaultId_AbnormalReceptionOnSfpToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The Optif is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to upper hop <OptIf ID>\n\nFAULT ID\n1971: EFaultId_AbnormalReceptionOnSfpToUpperHopAl\n\nMEANING\nThe optical interface is not working properly. There is abnormal signal reception from the upper hop FR. This fault is valid only for radio modules in chain configuration.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module. \n2. Reset the RF module. \n3. If those do not help, block and unblock the site. \n4. If those do not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAccess panel port(s) enabled\n\nFAULT ID\n234: EFaultId_AccessPanelPortEnaAl\n\nMEANING\nThe FlexiZone Micro BTS, Flexi Zone Access Point, or Flexi Zone SFN Antenna has detected that one or more access panel ports is enabled.\n\nThis state of elevated security risk is not expected in field conditions.\n\nINSTRUCTIONS\n1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, use SSH to disable access panel port(s) and/or physically inspect site installation.\n\n\n\n\nFAULT NAME\nALD port configuration failure\n\nFAULT ID\n4255: EFaultId_AldPortFailureAl\n\nMEANING\nThe Radio Module has detected switch configuration mismatch on the ALD port.\n\nINSTRUCTIONS\n1. Check the configuration of the ALD port.\n\n2. The alarm is cancelled only when the RF Module is reset, or the BTS is reset.\n\n\n\n\nFAULT NAME\nALD Port power failure\n\nFAULT ID\n4069: EFaultId_Rs485PowerFailureAl\n\nMEANING\nOBSAI interface:\nThe Radio Module has detected an over-current condition in the RS485 IUANT port.\nSome antenna line device is causing overload. Antenna line devices powered by the RS485 IUANT are out of		

Table 40-11 BASE_STATION_OPERATION_DEGRADED

Alarm	Attributes	Applicable major release
Name: BASE_STATION_OPERATION_DEGRADED (11519) Type: equipmentAlarm Package: racfl.BASE_STATION_OPERATION_DEGRADED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION OPERATION DEGRADED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION OPERATION DEGRADED\n\nA major fault (or faults) has occurred in the base station.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-11 BASE_STATION_OPERATION_DEGRADED (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see the source of the alarm and instructions fields of the corresponding alarms). \n\nBelow is the list of BTS fault(s) which might have caused this alarm in BTS FL16A/TL16A release. In case of earlier SW release and in case you need more detailed fault descriptions refer to LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n\nFAULT NAME\n2M external reference missing\n\nFAULT ID\n1899: EFaultId_ 2MExtRefMissAl\n\nMEANING\nThe reference clock monitoring has detected a signal loss of 2.048 MHz received from an external reference source, connected to Sync In interface of the System Module.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the alarm disappears.\n\n1. Check the cabling (connected to Sync In interface).\n\n2. Check if the 2.048 MHz reference source is working normally, and the 2.048 MHz signal is available.\n\n3. Replace the alarming module.\n\n\n\n\nFAULT NAME\nAddress mismatch in summing\n\nFAULT ID\n2019: EFaultId_Muksu_SsubMmAl\n\nMEANING\nThere is a baseband bus address mismatch in the summing. There are two possible causes:\n\n1. A configuration error (two different baseband units functioning) - after an acknowledgement, the fault returns.\n\n2. Data corruption on the bus - appears once when an unsynchronized data is sent by the baseband.\n\nINSTRUCTIONS\nCheck the antenna mapping to the local cells in the commissioning file.\n\n\n\n\nFAULT NAME\nAntenna link is down\n\nFAULT ID\n476: EFaultId_Rp3BusError\n\nMEANING\nThe antenna (RP3) link is down. The transmitter or receiver drops from synchronization.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Restart the BTS.\n2. If that does not help, replace the alarming module. \n\nFlexi BTS FDD/TDD: In case the FSP is causing the alarm, replace the FSM because the alarm is related to the fixed FSP inside the FSM. \n\nFlexi BTS FDD/TDD, AirScale BTS FDD/TDD: If FBBx or ABIx is causing the alarm, replace the FBBx or ABIx.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone, Flexi Zone SFN Antenna: Replace the Flexi Zone Micro BTS, Flexi Zone Access Point, or Flexi Zone SFN Antenna.\n\n\n\n\ nFAULT NAME\nBaseband bus configuration of <x> was rejected\n\nFAULT ID\n1811: EFaultId_BbBus_ConfFailedAl\n\nMEANING\ nThe baseband-bus-related configuration of <x> has been rejected by the HW SW, DSP, or RF SW.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nReplace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Download the correct configuration.\n2. Reset the BTS.\n3. Replace the BTS.\n\nFlexi Zone:\n1. Download the correct configuration.\n2. Reset the Flexi Zone Access Point from the BTSSM.\n3. Replace the Flexi Zone Access Point.\n\nFlexi Zone SFN Antenna:\n1. Download the correct configuration.\n2. Reset the Flexi Zone SFN Antenna from the BTSSM.\n3. Replace the Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nBaseband bus failure\n\nFAULT ID\n3020: EFaultId_BaseBandBusFailure\n\nMEANING\nThe Flexi BTS has detected an abnormal operation or a failure in the BTS\ninternal or external (optical link) baseband bus. The failure cannot be\nattributed to a specific module and there are several possible fault sources.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the other active BTS faults and act accordingly.\n\n2. Check the cables between the System Module and RF Module.\n\n3. Reset the RF Module and/or System Module, depending on the alarm source:\n a. Reset the RF Module by blocking and unblocking it.\n b. Reset the System Module by blocking and unblocking it.\n\n4. Replace the alarming RF Module.\n\n5. If the System Module is the source, or replacing the RF Module does not clear the fault situation, replace the alarming System Module.\n\n\n\n\nFAULT NAME\nBB bus reception error (summing device)\n\nFAULT ID\n2016: EFaultId_Muksu_SMTimeOffAl\n\nMEANING\nThe master frame in the received baseband bus frame is not in the correct place related to the internally-generated master frame pulse. Either the frame has been set into the wrong place (PI delay), or the data itself is in the wrong place.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module, the cable between the FBBx/ABIx module and the RF module, and the cable between the system module and the FBBx module.\n\n2. Replace the unit that causes the alarm (system module or FBBx/ABIx).\n\n\n\n\nFAULT NAME\nBB bus transmission error\n\nFAULT ID\n2017: EFaultId_Muksu_SRx10b8bAl\n\nMEANING\nA decoding error has been detected in the baseband internal link. The data packet is lost, or the content is corrupted.\n\nThis situation also occurs when the links are not synchronized with each other.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module, and the cable between the FBBx/ABIA module and the RF module.\n\n2. Reset the system module.\n\n3. Replace the alarming module (system module).\n\n\n\n\nFAULT NAME\nBTS file error\n\nFAULT ID\n1802: EFaultId_FileRequestFlashAl\n\nMEANING\nA software download to FSP, DSP, ABIx or FR has failed.\n\nINSTRUCTIONS\nNote: Perform the following steps in the listed order until the fault disappears:\n\n1. Use BTS Site Manager to perform a full commissioning to the BTS using the NetAct backup upload SCF file as template.\n\n2. Download two different software packages so that the faulty file is removed from the BTS.\n\n3. Download the software again.\n\n4. Replace the System Module.\n\n\n\n\nFAULT NAME\nBTS internal SW management problem\n\nFAULT ID\n3090: EFaultId_ BtsInternalSwManagementProblem\n\nMEANING\nA software update to a module or sub-assembly has failed, or a corrupted SW file has been detected in the FLASH.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears:\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Check the other active BTS faults. If the ROM disk is corrupted, change the alarming module.\n2. Reset the RF Module and/or System Module (depending on the fault source) by blocking/unblocking it.\n3. Update and activate the SW to the BTS.\n4. Check the SW files.\n5. Replace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Check the other active Flexi Zone Micro BTS or Flexi Zone Access Point faults. If the ROM disk is corrupted, change the Flexi Zone Micro BTS or Flexi Zone Access Point.\n2. Reset the Flexi Zone Micro BTS or Flexi Zone Access Point by blocking/unblocking it.\n3. Update and activate the SW to the BTS.\n4. Check the SW files.\n\nFlexi Zone:\n1. Check the other active Flexi Zone Access Point faults. If the ROM disk is corrupted, change the Flexi Zone Access Point.\n2. Reset the Flexi Zone Access Point to trigger new SW load.\n3. Check the SW files.\n\nFlexi Zone SFN Antenna:\n1. Check the other active Flexi Zone SFN Antenna faults. If the ROM disk is corrupted, change the Flexi Zone SFN Antenna.\n2. Reset the Flexi Zone SFN Antenna to trigger new SW load.\n3. Check the SW files.\n\n\n\n\nFAULT NAME\nBTS master clock tuning failure\n\nFAULT ID\n1818: EFaultId_Ov_OscAl\n\nMEANING\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD: \nThe OCXO adjustment area is reaching its limit value. The DAC word value of the OCXO is less than or equal to the Min.OcxoControlValue.Alarm.Set value specified in BPF, or greater than or equal to the Max.OcxoControlValue.Alarm.Set value specified in BPF.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone SFN Antenna:\nThe master clock frequency is tuned to within 5% of its minimum or maximum offset.		

Table 40-12 BASE_STATION_TRANSMISSION_ALARM

Alarm	Attributes	Applicable major release
Name: BASE_STATION_TRANSMISSION_ALARM (11520) Type: communicationsAlarm Package: racfl.BASE_STATION_TRANSMISSION_ALARM Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BASE STATION TRANSMISSION ALARM Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BASE STATION TRANSMISSION ALARM\n\nA transmission fault (or faults) has occured in the BTS. This alarm is an encapsulation alarm that is used to transfer the Flexi Transport Submodule (FTM) alarm data over the BTS O&M connection through iOMS to NetAct. In NetAct this alarm is shown in opened format. This means that the alarm number, alarm text, and supplementary information are shown in the original FTM format. Check the reason for the fault from the supplementary information fields and supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-12 BASE_STATION_TRANSMISSION_ALARM (continued)

Alarm	Attributes	Applicable major release
Remedial action: FAULT NAME\n$Protocol Timing source lost [on unit $U] [, interface $IF]\n\nFAULT ID\n61059: FTM_TIMING_ SOURCE_LOS\n\nMEANING\nOne of the synchronization sources in the configured priority list is unavailable.\nThis can be the primary or the secondary clock source.\n\nIn the alarm: Protocol can be PDH, Timing over Packet (ToP), and Synchronuous ethernet.\n\nUnit Number is optional:\n- For PDH and Synchronous Ethernet, Unit number is 0 or 1.\n- It is not present for Timing Over Packet(TOP).\n\ nThe interface value is optional:\n- For PDH, the value range depends on the hardware unit type: 1-16.\n- For Synchonuous Ethernet, the value range is 1-3.\n- It is not present for Timing over Packet.\n\nINSTRUCTIONS\nUse BTS Site Manager to check which interfaces have been configured as\nsynchronization sources. For all interfaces, do as follows:\n\n1. Check that the cables are connected to the correct connectors.\n2. Check whether the interface at the far end is switched on.\n3. Check whether there are active alarms at the far end. If there are,\nfollow the instructions on handling those alarms.\n4. Connect a loop cable and check whether the alarm disappears to verify that the hardware of the interface unit works correctly.\n\nMonitor the quality of the received clock.\n\n\n\n\ nFAULT NAME\nAIS on unit $U, interface $IF\n\nFAULT ID\n61151: FTM_AIS\n\nMEANING\nAlarm indication signal is received. This signal is generated by an intermediate PDH device in the forward direction because it detects a problem in its received signal.\n\nAll other transmission alarms related to this signal are suppressed.\n\nProbable cause: There is a transmission problem somewhere in the intermediate network, and AIS is sent instead of user traffic.\n\nINSTRUCTIONS\nCheck the intermediate transmission network for alarms indicating the root cause and follow the instructions for handling these alarms.\n\n\n\n\nFAULT NAME\nAutomatic BTS Operator Certificate retrieval unsuccessful\n\nFAULT ID\n61510: NO_CERTIFICATE\n\nMEANING\nA requested certificate could not be retrieved from the certificate authority (CA).\nA requested certificate could not be renewed from the certificate authority (CA).\n\nA requested certificate could not be retrieved as the number of certificates received from repository server (RA) or certificate authority (CA) are more than expected.\n\nA requested certificate could not be stored in the remaining storage available on the BTS. Operator cleanup (e.g. via site manager or NetAct) of old, unused trust chains may be required.\n\nINSTRUCTIONS\nProvide the certificate.\n\n\n\n\nFAULT NAME\nAuto-negotiation mismatch, on unit $U, Ethernet interface $IF\n\nFAULT ID\n61607: AUTO NEGO MIS MATCH\n\nMEANING\ nThis alarm indicates that there is a mismatch between the BTS configuration and the auto-negotiation result.\n\nINSTRUCTIONS\ nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nTry with local management or site support equipment.\n\ nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone:\nConfirm that the Ethernet Synchronization master/slave settings are correct on the Flexi Zone Micro BTS or Flexi Zone Access Point and backhaul equipment. \nNote: The Flexi Zone Micro BTS and Flexi Zone Access Point only support slave mode.\n\n\n\n\nFAULT NAME\nBFD $session down, egress, $sourceIP to $destinationIP\n\ nFAULT ID\n61606: BFD DOWN Egress\n\nMEANING\nThe alarm is raised if the alarm is enabled, the BFD state of the session is not "AdminDown", and the BFD packet from the far end contains the diagnostic code =" "Control Detection Time Expired" and no ingress alarm is present.\n\nINSTRUCTIONS\nCheck the BFD configuration at the local end.\n\n\n\n\n\nFAULT NAME\nBFD $session down, ingress, $sourceIP to $destinationIP\n\nFAULT ID\n61605: BFD DOWN Ingress\n\nMEANING\nThe alarm is raised if the alarm is enabled, the BFD state for the session is not "AdminDown", and nevertheless, no BFD packet is received at the local end during the detection time.\n\nINSTRUCTIONS\n1. Check the network between both BFD peers for physical link failures or misconfigurations.\n\n2. Check if the BFD functionality in the peer is switched on and that the configurations of the BFD peers match.\n\n\n\n\nFAULT NAME\nBFD group $bfdGrpId down\n\nFAULT ID\n61022: BFD DOWN\n\nMEANING\nThe alarm is raised if the BFD service is not available on the BTS for all BFD sessions belonging to that BFD group.\n\nINSTRUCTIONS\n1. Check if the far end has BFD switched on.\n2. Check the cabling and network connections of the far end.\n\n\n\n\nFAULT NAME\nBluetooth enabled\n\nFAULT ID\n61520: BLUETOOTH_ENABLED\n\nMEANING\nIf the actBluetoothTransAlarm parameter allows, this fault is raised to indicate that the bluetooth has been enabled because of any of the following:\n- The bluetooth config mode set to explicitly enabled\n- The bluetooth config mode AutoFallback logic, which automatically enables the bluetooth upon loss of connection to the iOMS or NetAct\n\ nINSTRUCTIONS\n1. Determine if the bluetooth should be enabled.\n2. If this action is unexpected, disable the bluetooth.\n\n\n\n\ nFAULT NAME\nBluetooth network connected\n\nFAULT ID\n61522: BLUETOOTH_CONNECTED\n\nMEANING\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected a bluetooth network connection.\n\nINSTRUCTIONS\n1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.\n\n\n\n\nFAULT NAME\nBluetooth Paired\n\nFAULT ID\n61521: BLUETOOTH_PAIRED\n\nMEANING\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected a successful pairing.\n\nINSTRUCTIONS\n1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.\n\n\n\n\nFAULT NAME\nBluetooth repeated authentication failure\n\nFAULT ID\n61523: BLUETOOTH_AUTH_FAIL\n\nMEANING\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected repeated bluetooth authentication failures. This could signal that a passkey or pin guessing attack is ongoing.\n\nINSTRUCTIONS\n1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.\n\n\n\n\nFAULT NAME\nBTS and/or peer trust anchor expired or due to expire\n\nFAULT ID\n61618: TRUST_ANCHOR_EXPIRING\n\nMEANING\nThe network element stores trust anchors for its own trust chain and for peers. When its own or any trust anchors are about to expire or are expired, this alarm is sent.\n\n\nINSTRUCTIONS\nUpdate the trust anchors.\n\n\n\n\nFAULT NAME\nBTS booted at $date due to $RCause\n\nFAULT ID\n61006: FTM_RESET\n\nMEANING\nThe transport part of the BTS has been reset at the date and time given in the notification.\n\n1. FSMr2 supports the following cause for the reset:\n\n"trs power-on reset": Cold start \n"trs watchdog reset": System overload\n"trs startup failure": Failure during startup \n"trs software failure": Software failure\n"trs management reset": Reset triggered by management interface\n"trs fallback": Fallback executed\n\nFSMr3/AirScale supports the following cause for the reset:\n\n"trs power-on reset": Cold start\n"trs watchdog reset": System overload\n"trs software failure": Software failure\n"trs management reset": Reset triggered by management interface\n"trs spurious reset": Reset reason detection failed\n\n2. The "$date" format is the local time stamp (GMT+/-xx:xx). For example: 2014-04-12 00:51:26 GMT+0530\n\nINSTRUCTIONS\nNo actions are required.\n\n\n\n\nFAULT NAME\nBTS Local OAM user account $A has been locked\n\nFAULT ID\n61642: FTM_SECURITY_USER_ ACCOUNT\n\nMEANING\nA specific BTS local operator account has been locked.\nThe number of failed login attempts for a BTS local operator account has exceeded the threshold, and the account has been locked on the BTS. No further logins are permitted for this account until it is unlocked.\n\nINSTRUCTIONS\nCheck the validity of the username and password of the account.\n\n\n\n\nFAULT NAME\nBTS reset required\n\nFAULT ID\n61010: FTM_BTS_RESET_REQUIRED\n\nMEANING\nA change to the BTS IP settings has been received from the BTS Site Manager. The BTS should be restarted to activate the change.\n\nINSTRUCTIONS\nReset the BTS when all the required BTS IP settings have been set.\n\n\n\n\nFAULT NAME\nCCM fault level $ prio $p cause $c\n\nFAULT ID\n61410:			

Table 40-13 BFD_DOWN

Alarm	Attributes	Applicable major release
Name: BFD_DOWN (11521) Type: communicationsAlarm Package: racfl.BFD_DOWN Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BFD DOWN Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BFD DOWN\n\nThe alarm is raised if the BFD service is not available on the BTS for all BFD sessions belonging to that BFD group.\n\nThe communication link between the BTS and the BFD peer is defective. No communication is possible.\n\nThe system cancels the alarm autonomously once the BFD functionality is available again.		
Remedial action: 1. Check if the far end has BFD switched on.\n2. Check the cabling and network connections of the far end.		

Table 40-14 BFD_DOWN_Egress

Alarm	Attributes	Applicable major release
Name: BFD_DOWN_Egress (11522) Type: communicationsAlarm Package: racfl.BFD_DOWN_Egress Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BFD DOWN Egress Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BFD DOWN Egress\n\nThe alarm is raised if the alarm is enabled, the BFD state of the session is not 'AdminDown', and the BFD packet from the far end contains the diagnostic code =" 'Control Detection Time Expired' and no ingress alarm is present.\n\nThe communication link between the BTS and the BFD peer is defective. No communication is possible.\n\nThe system cancels the alarm autonomously once the local BFD session receives error-free BFD packets from its BFD peer."		
Remedial action: Check the BFD configuration at the local end.		

Table 40-15 BFD_DOWN_Ingress

Alarm	Attributes	Applicable major release
Name: BFD_DOWN_Ingress (11523) Type: communicationsAlarm Package: racfl.BFD_DOWN_Ingress Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BFD DOWN Ingress Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BFD DOWN Ingress\n\nThe alarm is raised if the alarm is enabled, the BFD state for the session is not 'AdminDown', and nevertheless, no BFD packet is received at the local end during the detection time.\n\nThe communication link between the BTS and the BTS peer is defective, or the peer itself is defective. No communication is possible.\n\nThe system cancels the alarm autonomously if the local BFD peer receives BFD packets from the remote BFD peer.		
Remedial action: 1. Check the network between both BFD peers for physical link failures or misconfigurations.\n\n2. Check if the BFD functionality in the peer is switched on and that the configurations of the BFD peers match.		

Table 40-16 BLUETOOTH_AUTH_FAIL

Alarm	Attributes	Applicable major release
Name: BLUETOOTH_AUTH_FAIL (11524) Type: communicationsAlarm Package: racfl.BLUETOOTH_AUTH_FAIL Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BLUETOOTH_AUTH_FAIL Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BLUETOOTH_AUTH_FAIL\n\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected repeated bluetooth authentication failures. This could signal that a passkey or pin guessing attack is ongoing.\n\nTo prevent a DoS attack, this fault does not disable the bluetooth. Instead, the offending devices are subjected to exponential backoff for authentication attempts and might be blacklisted.\n\n		
Remedial action: 1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.		

Table 40-17 BLUETOOTH_CONNECTED

Alarm	Attributes	Applicable major release
Name: BLUETOOTH_CONNECTED (11525) Type: communicationsAlarm Package: racfl.BLUETOOTH_CONNECTED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BLUETOOTH_CONNECTED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BLUETOOTH_CONNECTED\n\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected a bluetooth network connection.\n\nNone\n\n		
Remedial action: 1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.		

Table 40-18 BLUETOOTH_ENABLED

Alarm	Attributes	Applicable major release
Name: BLUETOOTH_ENABLED (11526) Type: communicationsAlarm Package: racfl.BLUETOOTH_ENABLED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BLUETOOTH_ENABLED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BLUETOOTH_ENABLED\n\nIf the actBluetoothTransAlarm parameter allows, this fault is raised to indicate that the bluetooth has been enabled because of any of the following:\n- The bluetooth config mode set to explicitly enabled\n- The bluetooth config mode AutoFallback logic, which automatically enables the bluetooth upon loss of connection to the iOMS or NetAct\n\nAs a risk mitigation, this fault warns the operator that the bluetooth is enabled. While the bluetooth is enabled, the site is open to wireless local maintenance over bluetooth.\n\n		
Remedial action: 1. Determine if the bluetooth should be enabled.\n2. If this action is unexpected, disable the bluetooth.		

Table 40-19 BLUETOOTH_PAIRED

Alarm	Attributes	Applicable major release
Name: BLUETOOTH_PAIRED (11527) Type: communicationsAlarm Package: racfl.BLUETOOTH_PAIRED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: BLUETOOTH_PAIRED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: BLUETOOTH_PAIRED\n\nThe Flexi Zone Micro BTS or Flexi Zone Access Point has detected a successful pairing.\n\nNone\n\n		
Remedial action: 1. Determine if this event is expected. Investigate audit logs as necessary.\n2. If this action is unexpected, disable the bluetooth.		

Table 40-20 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • FL16A
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 40-21 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • FL16A
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 40-22 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • FL16A
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 40-23 BTSHardwareResynchronization

Alarm	Attributes	Applicable major release
Name: BTSHardwareResynchronization (11472) Type: configurationAlarm Package: netw.BTSHardwareResynchronization Raised on class: netw.NetworkElement	Severity: major Specific problem: Hardware Resynchronization Failure. Implicitly cleared: true Default probable cause: FILE_ERROR	Release: • FL16A
Description: The alarm is raised when the hardware configuration resynchronization failed. The detail of the error is set in the additional information of the alarm.		
Remedial action: Investigation is required to resolve the following possible scenarios: the BTS or OMS is unreachable (including underlying transport network issue); loss of connectivity to the BTS or OMS during transfer; CORBA and HTTP security credential issues; OMS or BTS internal errors. Once the problem solved in the system, the BTS hardware configuration has to be resynchronized from SAM using BTS full resynchronization.		

Table 40-24 CELL_FAULTY

Alarm	Attributes	Applicable major release
Name: CELL_FAULTY (11528) Type: qualityOfServiceAlarm Package: racfl.CELL_FAULTY Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: CELL FAULTY Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-24 CELL_FAULTY (continued)

Alarm	Attributes	Applicable major release
Description: CELL FAULTY\n\nA critical fault (or faults) has occurred in a unit (or units) that belong to the sector indicated in the alarm.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-24 CELL_FAULTY (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see the source of the alarm and instructions fields of the corresponding alarms). \n\nBelow is the list of BTS fault(s) which might have caused this alarm in BTS FL16A/TL16A release. In case of earlier SW release and in case you need more detailed fault descriptions refer to LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n----------\n\nFAULT NAME\nAbnormal CPRI interface to next hop <OptIf ID>\n\nFAULT ID\n1974: EFaultId_AbnormalCpriInterfaceToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThe CPRI transmission is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The Optif is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is causing the alarm (connected to the faulty optical link, to the end farther from the system module).\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to next hop <OptIf ID>\n\nFAULT ID\n1973: EFaultId_AbnormalReceptionOnSfpToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The Optif is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to upper hop <OptIf ID>\n\nFAULT ID\n1971: EFaultId_AbnormalReceptionOnSfpToUpperHopAl\n\nMEANING\nThe optical interface is not working properly. There is abnormal signal reception from the upper hop FR. This fault is valid only for radio modules in chain configuration.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module. \n2. Reset the RF module. \n3. If those do not help, block and unblock the site. \n4. If those do not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAntenna calibration error caused by transmission path failure \n\nFAULT ID\n1987: EFaultId_CalibrationErrorCausedByTransmissionPathFailureAl\n\nMEANING\nAntenna calibration has failed on at least 3 antennas because of a transmission path failure.\n\nThe path means all units between the signaling processor (DSP) and the antenna inside the radio module.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the fault is resolved:\n1. Check if other alarms are not reported at the same time. If other alarms are reported, follow the necessary instructions to clear them.\n2. Reset the radio module, which is the fault source.\n3. Reset the BTS.\n4. Replace the radio module, which is the fault source.\n\n\n\n\nFAULT NAME\nAntenna Line Device failure\n\nFAULT ID\n3100: EFaultId_AntennaLineFailure\n\nMEANING\nThe System Module, or the device itself, has detected an abnormal operation or a failure in the antenna line device.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the antenna line and antenna line devices. Ensure that the antenna line connectors are in the right torque.\n\n2. Block and unblock the alarming RF module to reset it.\n\n3. Replace the faulty parts and/or devices along the antenna line.\n\n4. Replace the RF Module.\n\n\n\n\nFAULT NAME\nAntenna line failure\n\nFAULT ID\n1836: EFaultId_ALOvercurrentAl\n\nMEANING\nThe radio module or filter has detected overcurrent on the antenna line. The antenna line might be damaged (short-circuited), or some antenna line device is causing overload. All antenna line devices powered by the antenna line are out of order.\n\nINSTRUCTIONS\n1. Check the antenna line and antenna line devices. Fix or replace the faulty parts or devices.\n2. For CPRI-A radios, the fault might cancel automatically if the fault condition is cleared within 1 minute of detection. For some CPRI-A radios, the fault might cancel automatically after the fault condition is cleared regardless of when the condition is cleared. If the fault is not canceled automatically, the fault is canceled when the RF module is blocked or unblocked, or when the RF module or the BTS is reset. \n3. For all other radios, the fault is canceled only when the RF module or the BTS is reset.\n\n\n\n\nFAULT NAME\nAntenna line faulty \n\nFAULT ID\n4045: EFaultId_AntennaLineFaultyAl\n\nMEANING\nAn alarm message has been received from the antenna line. The antenna line is faulty.\n\nINSTRUCTIONS\nThe following instructions should be performed on the master RAT side:\n\n1. Check the antenna line and antenna line device that causes the alarm.\n2. Fix or replace the faulty parts or devices.\n3. Perform a radio module reset (only the master RAT in sharing mode can request for such an operation to be performed).\n\n\n\n\nFAULT NAME\nAntenna line switched off due to high VSWR\n\nFAULT ID\n1957: EFaultId_AntennaLineSwitchedOffAl\n\nMEANING\nTx in the RF module has been switched off to protect the radio module hardware, which might be damaged because of high-reflection (VSWR) conditions.\n\nINSTRUCTIONS\n1. The VSWR measured at the RF (transmitter) exceeds values that are acceptable by the RF module.\n2. Check the impedance matching of the Antenna Line System (replace elements that cause mismatch).\n3. To check if the above-mentioned steps have solved the problem, reset the RF module.\n\n*Forcing the RF HW to work under such conditions might result in permanent damage to the RF HW.\n\n\n\n\nFAULT NAME\nAntenna link is down\n\nFAULT ID\n476: EFaultId_Rp3BusError\n\nMEANING\nThe antenna (RP3) link is down. The transmitter or receiver drops from synchronization.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Restart the BTS.\n2. If that does not help, replace the alarming module. \n\nFlexi BTS FDD/TDD: In case the FSP is causing the alarm, replace the FSM because the alarm is related to the fixed FSP inside the FSM. \n\nFlexi BTS FDD/TDD, AirScale BTS FDD/TDD: If FBBx or ABIx is causing the alarm, replace the FBBx or ABIx.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone, Flexi Zone SFN Antenna: Replace the Flexi Zone Micro BTS, Flexi Zone Access Point, or Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nBaseband bus configuration of <x> was rejected\n\nFAULT ID\n1811: EFaultId_BbBus_ConfFailedAl\n\nMEANING\nThe baseband-bus-related configuration of <x> has been rejected by the HW SW, DSP, or RF SW.\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nReplace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Download the correct configuration.\n2. Reset the BTS.\n3. Replace the BTS.\n\nFlexi Zone:\n1. Download the correct configuration.\n2. Reset the Flexi Zone Access Point from the BTSSM.\n3. Replace the Flexi Zone Access Point.\n\nFlexi Zone SFN Antenna:\n1. Download the correct configuration.\n2. Reset the Flexi Zone SFN Antenna from the BTSSM.\n3. Replace the Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nBaseband bus failure\n\nFAULT ID\n3020: EFaultId_BaseBandBusFailure\n\nMEANING\nThe Flexi BTS has detected an abnormal operation or a failure in the BTS\ninternal or external (optical link) baseband bus. The failure cannot be\nattributed to a specific module and there are several possible fault sources.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the other		

Table 40-25 CELL_NOTIFICATION

Alarm	Attributes	Applicable major release
Name: CELL_NOTIFICATION (11529) Type: qualityOfServiceAlarm Package: racfl.CELL_NOTIFICATION Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: CELL NOTIFICATION Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: CELL NOTIFICATION\n\nA minor fault (or faults) has occurred in a unit (or units) that belong to the sector indicated in the alarm.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-25 CELL_NOTIFICATION (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see the source of the alarm and instructions fields of the corresponding alarms). \n\nBelow is the list of BTS fault(s) which may have caused this alarm in BTS FL16A/TL16A release. In case of earlier SW release and in case you need more detailed fault descriptions refer to LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n\n----------\n\nFAULT NAME\nAntenna Line Device failure\n\nFAULT ID\n3100: EFaultId_AntennaLineFailure\n\nMEANING\nThe System Module, or the device itself, has detected an abnormal operation or a failure in the antenna line device.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the antenna line and antenna line devices. Ensure that the antenna line connectors are in the right torque.\n\n2. Block and unblock the alarming RF module to reset it.\n\n3. Replace the faulty parts and/or devices along the antenna line.\n\n4. Replace the RF Module.\n\n\n\n\nFAULT NAME\nAntenna Line Device Operation Failure\n\nFAULT ID\n1871: EFaultId_BusyAl\n1872: EFaultId_FormatErrorAl \n1873: EFaultId_UnsupportedProcedureAl \n1874: EFaultId_OutOfRangeAl \n\nMEANING\nThe device is not working properly, the configuration is not valid, or a given parameter is incorrect.\n\nINSTRUCTIONS\n1. Check the functionality of the antenna line device.\n\n2. Check the compatibility between the antenna line device and the BTS.\n\n3. Check that the given parameters are in the valid range.\n\n\n\n\nFAULT NAME\nAntenna line device SW download failure\n\nFAULT ID\n4047: EFaultId_FileCrcErrorAl\n4048: EFaultId_FileContentErrorAl\n\nMEANING\nAn SW download to an antenna line device has failed because of an incorrect checksum or file format.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears:\n\n1. Check the SW package.\n2. Download the SW to the antenna line device again.\n\n\n\nFAULT NAME\nAntenna line failure\n\nFAULT ID\n1836: EFaultId_ALOvercurrentAl\n\nMEANING\nThe radio module or filter has detected overcurrent on the antenna line. The antenna line might be damaged (short-circuited), or some antenna line device is causing overload. All antenna line devices powered by the antenna line are out of order.\n\nINSTRUCTIONS\n1. Check the antenna line and antenna line devices. Fix or replace the faulty parts or devices.\n2. For CPRI-A radios, the fault might cancel automatically if the fault condition is cleared within 1 minute of detection. For some CPRI-A radios, the fault might cancel automatically after the fault condition is cleared regardless of when the condition is cleared. If the fault is not canceled automatically, the fault is canceled when the RF module is blocked or unblocked, or when the RF module or the BTS is reset. \n3. For all other radios, the fault is canceled only when the RF module or the BTS is reset.\n\n\n\n\nFAULT NAME\nBaseband bus failure\n\nFAULT ID\n3020: EFaultId_BaseBandBusFailure\n\nMEANING\nThe Flexi BTS has detected an abnormal operation or a failure in the BTS\ninternal or external (optical link) baseband bus. The failure cannot be\nattributed to a specific module and there are several possible fault sources.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the other active BTS faults and act accordingly.\n\n2. Check the cables between the System Module and RF Module.\n\n3. Reset the RF Module and/or System Module, depending on the alarm source:\n a. Reset the RF Module by blocking and unblocking it.\n b. Reset the System Module by blocking and unblocking it.\n\n4. Replace the alarming RF Module.\n\n5. If the System Module is the source, or replacing the RF Module does not clear the fault situation, replace the alarming System Module.\n\n\n\n\nFAULT NAME\nBTS internal SW management problem\n\nFAULT ID\n3090: EFaultId_BtsInternalSwManagementProblem\n\nMEANING\nA software update to a module or sub-assembly has failed, or a corrupted SW file has been detected in the FLASH.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears:\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Check the other active BTS faults. If the ROM disk is corrupted, change the alarming module.\n2. Reset the RF Module and/or System Module (depending on the fault source) by blocking/unblocking it.\n3. Update and activate the SW to the BTS.\n4. Check the SW files.\n5. Replace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Check the other active Flexi Zone Micro BTS or Flexi Zone Access Point faults. If the ROM disk is corrupted, change the Flexi Zone Micro BTS or Flexi Zone Access Point.\n2. Reset the Flexi Zone Micro BTS or Flexi Zone Access Point by blocking/unblocking it.\n3. Update and activate the SW to the BTS.\n4. Check the SW files.\n\nFlexi Zone:\n1. Check the other active Flexi Zone Access Point faults. If the ROM disk is corrupted, change the Flexi Zone Access Point.\n2. Reset the Flexi Zone Access Point to trigger new SW load.\n3. Check the SW files.\n\nFlexi Zone SFN Antenna:\n1. Check the other active Flexi Zone SFN Antenna faults. If the ROM disk is corrupted, change the Flexi Zone SFN Antenna.\n2. Reset the Flexi Zone SFN Antenna to trigger new SW load.\n3. Check the SW files.\n\n\n\n\nFAULT NAME\nBTS SW download or activation failed\n\nFAULT ID\n29: EFaultId_FileCorruptionAl\n30: EFaultId_SwUpdateAl\n\nMEANING\nThe SW update to the BTS has failed. The error can be caused by a module reset during the SW update, a hardware problem in the module, or a corrupted flash file system.\n\n\n\nINSTRUCTIONS\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\n1. Retry the SW update.\n2. If other flash memory-related faults are active for the alarming module at the same time, replace the alarming module.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone Controller:\n1. Retry the SW update.\n2. If other flash memory-related faults are active for the BTS at the same time, replace the BTS.\n\nFlexi Zone Access Point:\n1. Retry the SW update by resetting the Flexi Zone Access Point using the BTS SM.\n2. If other flash memory-related faults are active for the Flexi Zone Access Point at the same time, replace the Access Point.\n\nFlexi Zone SFN Antenna:\n1. Retry the SW update by resetting the Flexi Zone SFN Antenna using the BTS SM.\n2. If other flash memory-related faults are active for the Flexi Zone SFN Antenna at the same time, replace the Flexi Zone SFN Antenna.\n\n\n\n\nFAULT NAME\nConfiguration error: <x>\n\nFAULT ID\n3070: EFaultId_ConfigurationError \n\nMEANING\nThere is a compatibility problem in the BTS HW/SW versions or the HW/HW configuration. Another possibility is that there is a mismatch in the BTS configuration.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears:\n\n1. Check the installed HW/SW version compatibility and the HW compatibility with the current BTS configuration.\n\n2. Check that the BTS cell parameters from the Network management system match\nthe BTS HW configuration (for example, frequency, power).\n\n3. Check the Network management system alarms for the alarming local cell (LCR).\n\n4. Recommission the BTS to ensure that all parameters are correctly configured.\n\n\n\n\nFAULT NAME\nCorrectable bit toggling error\n\nFAULT ID\n6700: EFaultId_CorrectableBitTogglingError\n\nMEANING\nA correctable bit toggling error is detected in DSP memory.\n\nINSTRUCTIONS\nThe fault doesn't require any special action because it was already autonomously corrected.\n\n\n\n\nFAULT NAME\nCritical bit toggling error\n\nFAULT ID\n6701: EFaultId_CriticalBitTogglingError\n\nMEANING\nA non-correctable, bit-toggling error has been detected in the critical DSP			

Table 40-26 CELL_OPERATION_DEGRADED

Alarm	Attributes	Applicable major release
Name: CELL_OPERATION_DEGRADED (11530) Type: qualityOfServiceAlarm Package: racfl.CELL_OPERATION_DEGRADED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: CELL OPERATION DEGRADED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: CELL OPERATION DEGRADED\n\nA major fault (or faults) has occurred in a unit (or units) that belong to the sector indicated in the alarm.\n\nCheck the reason for the fault from the supplementary text field of the alarm.\n\nThe effect of the fault on the functioning of the network element depends on the fault description. For more information, see base station fault descriptions in LTE System Libraries.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		

Table 40-26 CELL_OPERATION_DEGRADED (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify the configuration of a BTS by checking the commissioning, cabling and correct installation of the units/modules at the BTS. Make sure the environment does not cause the fault.\n\nBefore a unit/module is replaced at the BTS, the site should be reset to recover from any temporary faults which might have caused the malfunctioning of the unit/module. When an active alarm is a 'Start' alarm, a site reset is required to cancel the alarm. If the site reset or module block/unblock does not help, replace the faulty unit/module (see the source of the alarm and instructions fields of the corresponding alarms). \n\nBelow is the list of BTS fault(s) which might have caused this alarm in BTS FL16A/TL16A release. In case of earlier SW release and in case you need more detailed fault descriptions refer to LTE System Libraries. The BTS fault descriptions are also included in BTS SW release documentation. If that does not help, contact your local customer support. \n\n----------\n\nFAULT NAME\n10b8b coding error in optical interface device\n\nFAULT ID\n2004: EFaultId_OIC_LVDSRecAl\n\nMEANING\nThe fiber cable is experiencing interference; data transmission is faulty.\n\nA physical connection failure between the optical interface and the summing function has occurred.\n\nThe reason of the fault might be a low-quality or polluted SFP, or a low-quality optical cable used to connect radio module to system module/extension baseband module.\n\n\nINSTRUCTIONS\nNote: Perform the steps in the listed order until the fault is resolved.\n\n1. Reset the radio module behind the cable reported as the fault source by blocking/unblocking it. \n2. Reset the system module. \n3. Replace the SFP on the radio module port where the cable reported as fault source is terminated.\n4. Replace the SFP on the system module or extension baseband module port where the cable reported as fault source is terminated.\n5. Replace the optical cable reported as fault source.\n6. Replace the radio module behind the cable reported as fault source.\n7. If the system module reset helped but the fault is reported again after some time or if the actions mentioned above have not cleared the fault situation, replace the extension baseband module (if the fault is reported on the cable connected to the baseband module) or the system module (if the fault is reported on the cable connected to the system module).\n\n\n\n\nFAULT NAME\n3GPP/AISG communication administratively disabled\n\nFAULT ID\n4142: EFaultId_Communication3gppAdministrativelyDisabledAl\n\nMEANING\nThe HDLC link has been disabled for the reporting Antenna Line or IUANT port.\n\nINSTRUCTIONS\nEnable the parameter "Communication3gppEnabled" for the reporting Antenna Line to revert changes.\n\n\n\n\nFAULT NAME\nAbnormal CPRI interface to next hop <OptIf ID>\n\nFAULT ID\n1974: EFaultId_AbnormalCpriInterfaceToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThe CPRI transmission is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The OptIf is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is causing the alarm (connected to the faulty optical link, to the end farther from the system module).\n\n\n\n\nFAULT NAME\nAbnormal CPRI interface to upper hop <OptIf ID>\n\nFAULT ID\n1965: EFaultId_AbnormalCpriInterfaceToUpperHopAl\n\nMEANING\nThe optical interface does not work properly. CPRI transmission to the upper hop does not work properly.\n\nINSTRUCTIONS\nExecute the following steps in the ordered sequence. If any of the step does not help, execute the next one:\n\n1. Reset the radio module behind the cable reported as the fault source. \n2. Reset the system module. \n3. Replace the SFP on the radio module port where the cable reported as the fault source is terminated.\n4. Replace the SFP on the system module or the extension baseband module port where the cable reported as the fault source is terminated.\n5. Replace the optical cable reported as the fault source.\n6. Replace the radio module behind the cable reported as the fault source.\n7. If the actions mentioned above did not clear the faulty situation, replace the extension baseband module (if the fault is reported on the cable connected to the baseband module) or the system module (if the fault is reported on the cable connected to the system module).\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to next hop <OptIf ID>\n\nFAULT ID\n1973: EFaultId_ AbnormalReceptionOnSfpToNextHopAl\n\nMEANING\nThe optical interface is not working properly.\nThis fault is valid only for radio modules in a chain configuration.\nNote: The OptIf is from the perspective of the previous radio.\n\nINSTRUCTIONS\n1. Check the cables between the RF module that is reported as the fault source and the RF module that is closer to the system module or ABIA. \n2. Reset the RF module. \n3. If that does not help, block or unblock the site. \n4. If that does not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAbnormal reception on SFP to upper hop <OptIf ID>\n\nFAULT ID\n1971: EFaultId_AbnormalReceptionOnSfpToUpperHopAl\n\nMEANING\nThe optical interface is not working properly. There is abnormal signal reception from the upper hop FR. This fault is valid only for radio modules in chain configuration.\n\nINSTRUCTIONS\n1. Check the cables between the system module and the RF module. \n2. Reset the RF module. \n3. If those do not help, block and unblock the site. \n4. If those do not help, replace the RF module that is generating the alarm.\n\n\n\n\nFAULT NAME\nAddress mismatch in summing\n\nFAULT ID\n2019: EFaultId_Muksu_SsubMmAl\n\nMEANING\nThere is a baseband bus address mismatch in the summing. There are two possible causes:\n\n1. A configuration error (two different baseband units functioning) - after an acknowledgement, the fault returns.\n\n2. Data corruption on the bus - appears once when an unsynchronized data is sent by the baseband.\n\nINSTRUCTIONS\nCheck the antenna mapping to the local cells in the commissioning file.\n\n\n\n\nFAULT NAME\nAntenna line device configuration failure\n\nFAULT ID\n1888: EFaultId_AlConfigurationFailureAl\n\nMEANING\nAntenna Line Device is not properly configured.\nAntenna Line Device set-up fails, for example due to protocol error or interoperability problem.\n\nINSTRUCTIONS\n1. Check/correct the antenna line configuration.\n\n2. If that does not help, replace the antenna line device.\n\n\n\n\nFAULT NAME\nAntenna Line Device failure\n\nFAULT ID\n3100: EFaultId_AntennaLineFailure\n\nMEANING\nThe System Module, or the device itself, has detected an abnormal operation or a failure in the antenna line device.\n\nINSTRUCTIONS\nNote: Perform the steps below in the listed order until the BTS fault disappears.\n\n1. Check the antenna line and antenna line devices. Ensure that the antenna line connectors are in the right torque.\n\n2. Block and unblock the alarming RF module to reset it.\n\n3. Replace the faulty parts and/or devices along the antenna line.\n\n4. Replace the RF Module.\n\n\n\n\nFAULT NAME\nAntenna line device HW failure\n\nFAULT ID\n1847: EFaultId_HardwareErrorAl\n\nMEANING\nA hardware failure has been reported by ALD (RET, MHA).\n\nINSTRUCTIONS\n1. Reset the radio module to give a power-off reset to the antenna line devices.\n2. If step 1 does not help, replace the antenna line device.\n\n\n\n\nFAULT NAME\nAntenna line device missing software\n\nFAULT ID\n1848: EFaultId_WorkingSoftwareMissingAl \n\nMEANING\nThe unit is in download mode state. This fault is returned when an unsupported procedure occurs in download mode.\n\nINSTRUCTIONS\n1. Upload the correct SW to the device (if possible) or perform an ALD power reset (for example, by RF module reset).\n2. If that does not help, replace the antenna line device.\n\n\n\n\nFAULT NAME\nAntenna line device operation failure\n\nFAULT ID\n4239: EFaultId_AldOperationFailureAl\n\nMEANING\nThe radio module indicated an error upon execution of remote electrical tilt (RET)-related logical operation.\n\nINSTRUCTIONS\n1. Check the antenna		

Table 40-27 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • FL16A
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 40-28 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • FL16A
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 40-29 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 40-30 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 40-31 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 40-32 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • FL16A
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 40-32 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 40-33 CRL_Update_failure

Alarm	Attributes	Applicable major release
Name: CRL_Update_failure (11531) Type: communicationsAlarm Package: racfl.CRL_Update_failure Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: CRL Update failure Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: CRL Update failure\n\nThis alarm is raised if the BTS cannot update the Certificate Revocation List (CRL). Please refer to PDDB parameter 'CERTH::CRLInfo: CRLUpdateFailureReason' for failure reasons.\n\nThe Certificate Revocation List could not be updated. New revoked certificates\nremain unknown to the BTS.\n\nThe alarm is cleared after a successful update of the Certificate Revocation List in a new attempt.		
Remedial action: Execute general configuration checks:\n- Configuration of CMP server IP address and port, and DNS server IP address.\n- Configuration of routing entries towards remote peers.\n- Configuration of IPSec policies towards remote peers.\nCheck remote peers and intermediate network elements interconnections.\nCheck the LDAP connection towards the Certificate Revocation List server.\nCheck DNS names.\nCheck the size of the file at the Certificate Revocation List server.		

Table 40-34 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • FL16A
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 40-35 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 40-36 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 40-37 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • FL16A
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 40-38 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 40-39 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • FL16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 40-40 Ethernet_OAM_CCM_fault

Alarm	Attributes	Applicable major release
Name: Ethernet_OAM_CCM_fault (11558) Type: communicationsAlarm Package: racfl.Ethernet_OAM_CCM_fault Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: Ethernet OAM CCM fault Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-40 Ethernet_OAM_CCM_fault (continued)

Alarm	Attributes	Applicable major release
Description: Ethernet OAM CCM fault\n\nThe alarm is triggered whenever a service OAM error related to the transmission of Continuity Check Messages (CCM) persists on a given Ethernet interface as soon as one of the error conditions below occur:\n\nThe following alarms are defined:\n\n1. MDL_MISMATCH, priority 5 (highest priority): A CCM is received with an MDL that is lower than the highest configured one in the BTS, and does not match any of the configured ones.\nExample: CCM fault level - prio 5 cause MDL_MISMATCH\nNote: For MDL_MISMATCH cases, it might not be possible to display the local MDL where the fault was detected.\n\n2. MAID_MISMATCH priority 5: A CCM is received with an MDL that is configured in the BTS, but with an MAID that does not match any MA configured in the BTS on this MDL.\nExample: CCM fault level 5 prio 5 cause MAID_MISMATCH\n\n3. MAID_MISMATCH priority 5: A CCM is received with matching MDL and MAID, but the VLAN membership of the received frame does not match the VLAN configuration of the addressed MA.\nExample: CCM fault level 5 prio 5 cause MAID_MISMATCH\n\n4. ERR_CCM, priority 4: A CCM is received with known MDL and MAID, but the MEPID is not configured in the Remote MEP list of the MA.\nExample: CCM fault level 5 prio 4 cause REMOTEMEP_NOT_CONFIGURED\n\n5. ERR_CCM, priority 4: A CCM is received with known MDL, MAID, and MEPID, but the CCM interval coded in the received CCM does not match the interval configured in the BTS.\nEx: CCM fault level 5 prio 4 cause WRONG_CCM_INTERVAL \n\n6. REMOTE_CCM, priority 3: A CCM was not received for 3.5 intervals from at least one remote MEP in the MA.\nEx: CCM fault level 5 prio 3 cause REMOTE_CCM_DEFECT \n\n7. RDI_CCM, priority 1 (lowest priority): An RDI flag is detected in the CCM frames from one remote peer.\nExample: CCM fault level 5 prio 1 cause REMOTE_DEFECT_INDICATION\n\nThe alarm displays the following information:\n- Alarm Name\n- Alarm Priority\n- Alarm cause: if different sources produce the same alarm\n- MD level at which the alarm was detected\n\nThe transport connection toward the remote peer might be defective. Traffic might get lost.\n\nThe alarm is cleared when the CCM fault condition has stopped for at least 10 seconds, and no other CCM fault condition with a lower priority is active.		
Remedial action: 1. Check the cabling.\n2. Check the CCM configuration at the remote peer.		

Table 40-41 Ethernet_OAM_ETH_AIS_fault

Alarm	Attributes	Applicable major release
Name: Ethernet_OAM_ETH_AIS_fault (11559) Type: communicationsAlarm Package: racfl.Ethernet_OAM_ETH_AIS_fault Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: Ethernet OAM ETH_AIS_fault Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: Ethernet OAM ETH_AIS_fault\n\nWhen an MEP receives a valid ETH-AIS frame and AIS is enabled, it shall trigger an AIS alarm containing the following information:\n- receiving interface\n- MD level\n- Source MAC address\n\nNote:For FSMr3/AirScale unit types, interface is provided as: 'module type name' EIF 'interface number'. \nFor Flexi Zone Micro BTS, interface is provided as: EIF 'interface number'.\n\nThe transport connection towards the remote peer may be defective. Traffic may get lost.\n\nThe alarm is cancelled if no ETH_AIS message was received within 3.5 times the configurable ETH_AIS transmission period. This is either within 3.5 seconds or 3.5 minutes.		
Remedial action: 1. Check cabling.\n2. Check the configuration at the remote peer.		

Table 40-42 EXTERNAL_AL_1

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_1 (11532) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_1 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 1 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-42 EXTERNAL_AL_1 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 1\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 1.		

Table 40-43 EXTERNAL_AL_10

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_10 (11533) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_10 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 10 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 10\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 10.		

Table 40-44 EXTERNAL_AL_11

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_11 (11534) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_11 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 11 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 11\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 11.		

Table 40-45 EXTERNAL_AL_12

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_12 (11535) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_12 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 12 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-45 EXTERNAL_AL_12 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 12\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 12.		

Table 40-46 EXTERNAL_AL_13

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_13 (11536) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_13 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 13 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 13\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 13.		

Table 40-47 EXTERNAL_AL_14

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_14 (11537) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_14 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 14 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 14\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 14.		

Table 40-48 EXTERNAL_AL_15

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_15 (11538) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_15 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 15 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-48 EXTERNAL_AL_15 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 15\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 15.		

Table 40-49 EXTERNAL_AL_16

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_16 (11539) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_16 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 16 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 16\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 16.		

Table 40-50 EXTERNAL_AL_17

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_17 (11540) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_17 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 17 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 17\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 17.		

Table 40-51 EXTERNAL_AL_18

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_18 (11541) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_18 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 18 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-51 EXTERNAL_AL_18 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 18\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 18.		

Table 40-52 EXTERNAL_AL_19

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_19 (11542) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_19 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 19 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 19\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 19.		

Table 40-53 EXTERNAL_AL_2

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_2 (11543) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_2 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 2 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 2\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 2.		

Table 40-54 EXTERNAL_AL_20

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_20 (11544) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_20 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 20 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-54 EXTERNAL_AL_20 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 20\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 20.		

Table 40-55 EXTERNAL_AL_21

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_21 (11545) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_21 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 21 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 21\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 21.		

Table 40-56 EXTERNAL_AL_22

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_22 (11546) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_22 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 22 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 22\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 22.		

Table 40-57 EXTERNAL_AL_23

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_23 (11547) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_23 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 23 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-57 EXTERNAL_AL_23 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 23\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 23.		

Table 40-58 EXTERNAL_AL_24

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_24 (11548) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_24 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 24 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 24\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 24.		

Table 40-59 EXTERNAL_AL_25

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_25 (11549) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_25 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 25 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 25\n\nThis is an external user-defined alarm. The alarm is defined by the user\nin a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for\nthe user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when\nthe fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm\nnumber 25.		

Table 40-60 EXTERNAL_AL_26

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_26 (11550) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_26 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 26 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-60 EXTERNAL_AL_26 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 26\n\nThis is an external user-defined alarm. The alarm is defined by the user\nin a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for\nthe user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when\nthe fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm\nnumber 26.		

Table 40-61 EXTERNAL_AL_3

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_3 (11551) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_3 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 3 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 3\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 3.		

Table 40-62 EXTERNAL_AL_4

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_4 (11552) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_4 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 4 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 4\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 4.		

Table 40-63 EXTERNAL_AL_5

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_5 (11553) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_5 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 5 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-63 EXTERNAL_AL_5 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 5\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 5.		

Table 40-64 EXTERNAL_AL_6

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_6 (11554) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_6 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 6 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 6\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 6.		

Table 40-65 EXTERNAL_AL_7

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_7 (11555) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_7 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 7 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 7\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 7.		

Table 40-66 EXTERNAL_AL_8

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_8 (11556) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_8 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 8 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-66 EXTERNAL_AL_8 (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL AL 8\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 8.		

Table 40-67 EXTERNAL_AL_9

Alarm	Attributes	Applicable major release
Name: EXTERNAL_AL_9 (11557) Type: environmentalAlarm Package: racfl.EXTERNAL_AL_9 Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: EXTERNAL AL 9 Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: EXTERNAL AL 9\n\nThis is an external user-defined alarm. The alarm is defined by the user in a hardware database. Not applicable to Flexi Zone Micro platform and Flexi Zone platform.\n\nThe effect of the alarm depends on the purpose that was configured for the user-defined alarm input in the BTS.\n\nDo not cancel the alarm. The system automatically cancels the alarm when the fault has been corrected.		
Remedial action: The operation depends on the type of alarm that is used as external alarm number 9.		

Table 40-68 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • FL16A
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 40-69 FTM_AIS

Alarm	Attributes	Applicable major release
Name: FTM_AIS (11560) Type: communicationsAlarm Package: racfl.FTM_AIS Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_AIS Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_AIS\n\nAlarm indication signal is received. This signal is generated by an intermediate PDH device in the forward direction because it detects a problem in its received signal.\n\nAll other transmission alarms related to this signal are suppressed.\n\nProbable cause: There is a transmission problem somewhere in the intermediate network, and AIS is sent instead of user traffic.\n\nPossible impact on the connections over the interface in question:\n- no calls are possible\n- loss of remote management access to other network elements in the RAN\n\n		
Remedial action: Check the intermediate transmission network for alarms indicating the root cause and follow the instructions for handling these alarms.		

Table 40-70 FTM_BTS_RESET_REQUIRED

Alarm	Attributes	Applicable major release
Name: FTM_BTS_RESET_REQUIRED (11561) Type: communicationsAlarm Package: racfl.FTM_BTS_RESET_REQUIRED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_BTS_RESET_REQUIRED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_BTS_RESET_REQUIRED\n\nA change to the BTS IP settings has been received from the BTS Site Manager. The BTS should be restarted to activate the change.\n\nThe BTS does not take the new settings into use before a reset.\n\n		
Remedial action: Reset the BTS when all the required BTS IP settings have been set.		

Table 40-71 FTM_DPD

Alarm	Attributes	Applicable major release
Name: FTM_DPD (11562) Type: communicationsAlarm Package: racfl.FTM_DPD Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_DPD Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_DPD\n\nA dead peer has been detected in one of the IPsec associations of the FTM.\nThere is no response to the requests sent to the peer during the IKE SA setup, the IPsec SA setup, or during DPD.\n\nNote: When the IPSec backup tunnel feature is enabled, this alarm should not be raised because of failures when trying to set up primary IPSec tunnel in 'Secondary_Active_Probing_Primary' state.\n\nPossible reasons:\n- a cable is cut or there is no cable connected to the interface\n- the signal is excessively attenuated\n- the port at the connected far end node is switched off\n\nPossible effects:\n- No calls are possible.\n- loss of remote management access to other network elements in the RAN\n- loss of synchronization if the interface is used as a synchronization source\n- IKE SAs and IPSec SAs cannot be established or re-keyed.\n\nThe alarm condition for a protect policy does not exist anymore if the latest IKE message is answered by the peer.\n\nThe alarm is canceled as soon as the alarm condition does not exist for any protect policy.\n\nNote: When the IPSec backup tunnel feature is enabled, a DPD alarm caused by the primary tunnel failure is cleared when switch-over is successful for all primary tunnels (that is, all secondary tunnels are successfully established).\nSimilarly, any DPD alarm raised because of a secondary tunnel failure is cleared when switchback is successful for secondary tunnels (that is, all primary tunnels are successfully established).		

Table 40-71 FTM_DPD (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Check that the cables are connected to the correct connectors.\n2. Check that the interface at the far-end interface is switched on.\n3. Check whether there are active alarms at the far end. If there are, follow the instructions for handling those alarms.		

Table 40-72 FTM_EBER

Alarm	Attributes	Applicable major release
Name: FTM_EBER (11563) Type: communicationsAlarm Package: racfl.FTM_EBER Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_EBER Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_EBER\n\nExcessive bit error rate: The measured bit error rate exceeds the threshold value of BER-3 (10E-3).\n\nProbable causes:\n- the signal level is too low (optical connectors or cables are dirty, electrical connectors or cables are corroded)\n- the specified maximum length of the cable is exceeded\n- the connector is not properly connected to the unit\n- the receiver or the far-end transmitter has failed\n\nPossible impact:\n- slow management access to the WBTS and other network elements in the RAN\n- poor voice quality and data performance\n- if this interface is part of an IMA group, this IMA link should be temporarily suspended from operation\n\n		
Remedial action: 1. Clean the cables and connectors.\n\n2. Check that the connectors are properly connected to the unit.\n\n3. Check that the cable connected to the interface in question is not damaged and is within the specifications.\n\n4. Follow the signal in the network and check whether any other alarms concerning the fault are on (such as Laser End of Life). If they are, follow the instructions for handling those alarms.		

Table 40-73 FTM_FAULT_TOGGLING

Alarm	Attributes	Applicable major release
Name: FTM_FAULT_TOGGLING (11564) Type: communicationsAlarm Package: racfl.FTM_FAULT_TOGGLING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_FAULT_TOGGLING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_FAULT_TOGGLING\n\nAn FTM fault, for which the fault name appears in the Fault name field, is toggling in the FTM. Toggling fault condition is informed to the user with this new FTM fault. Toggling faults are supressed until the toggling alarm condition is cleared. Severity of this FTM fault is the same as the severity of the toggling FTM fault.\n\n\n\n		
Remedial action: 1. Check the fault name of the toggling FTM fault from the Fault name of\nthis fault.\n2. Follow the instructions of the toggling FTM fault to clear the problem.\n \nNote: Detailed information about the toggling frequency can be found in\nalarm history file, which can be downloaded using the BTS Site Manager. The log file is available with Snapshot.		

Table 40-74 FTM_LOF

Alarm	Attributes	Applicable major release
Name: FTM_LOF (11565) Type: communicationsAlarm Package: racfl.FTM_LOF Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_LOF Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_LOF\n\nLoss of frame: It is not possible to carry traffic on the interface referenced in the alarm text. All other transmission alarms related to this signal are suppressed.\n\nProbable cause for E1 interfaces: The interface at the far end is not configured to be a framed E1 interface.\n\nProbable cause for T1 interfaces: The interface at the far end is not configured to be a T1 interface.\n\nPossible impact on the connections over this interface:\n- no calls are possible\n- loss of remote management access to other network elements in the RAN\n- loss of synchronization if the interface is used as synchronization source\n\n		
Remedial action: E1 interfaces: Check that the interface type of the far-end interface is also configured to be a framed E1 interface. If this is not the case, reconfigure the interfaces so that they match each other.\n\nJT1 interfaces: Check that the interface type of the far-end interface is also configured to be a JT1 interface. If this is not the case, reconfigure the interfaces so that they match each other.		

Table 40-75 FTM_LOMF

Alarm	Attributes	Applicable major release
Name: FTM_LOMF (11566) Type: communicationsAlarm Package: racfl.FTM_LOMF Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_LOMF Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_LOMF\n\nLoss of multi-frame: The interface referenced in the alarm text has lost the multi-frame alignment.\n\nProbable cause: The interface type has not been configured to meet the framing of the interface at the far end. For E1 interfaces, the configuration of the far-end node should be E1 Multiframe.\n\nPossible impact: The performance management data collected on this interface becomes invalid.\n\n		
Remedial action: Check that the configured interface type matches the configured interface type of the far-end interface. If this is the case, the problem is somewhere in the transmission network.		

Table 40-76 FTM_LOS

Alarm	Attributes	Applicable major release
Name: FTM_LOS (11567) Type: communicationsAlarm Package: racfl.FTM_LOS Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_LOS Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-76 FTM_LOS (continued)

Alarm	Attributes	Applicable major release
Description: FTM_LOS\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD/TDD:\nNo signal is received on the interface referenced in the alarm text. All other transmission alarms related to this signal are suppressed.\n\nProbable causes for Ethernet interfaces:\n- a cable is cut, or there is no cable connected to the interface\n- the electrical signal is excessively reduced\n- the port at the connected far-end node is switched off\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nNo signal is received on the interface referenced in the alarm text. All other transmission alarms related to this signal are suppressed.\n\nProbable causes for Ethernet interfaces:\n- a cable is cut, or there is no cable connected to the interface\n- the electrical signal is excessively reduced\n- the port at the connected far-end node is switched off\n\nThe fault is generated only when the interface is not configured as LMP (that is, generated only when the interface is configured as the primary BH port, or when daisy chaining (enableLayer2Switching) is enabled).\n\nPossible impacts on the connections over this interface are:\n- no calls are possible\n- loss of remote management access to other network elements in the RAN\n- loss of synchronization if the interface is used as a synchronization source\n\n		
Remedial action: 1. Check that the cables are connected to the correct connectors.\n\n2. Check that the interface at the far-end interface is switched on.\n\n3. Check whether there are active alarms at the far end. If there are, follow the instructions for handling those alarms.\n\n4. Connect a loop cable and check whether the alarm disappears to verify that the hardware of the interface unit works correctly.		

Table 40-77 FTM_RDI

Alarm	Attributes	Applicable major release
Name: FTM_RDI (11568) Type: communicationsAlarm Package: racfl.FTM_RDI Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_RDI Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_RDI\n\nRemote defect indication: It is sent by the intermediate or the far-end equipment because it detects a serious fault in the received signal.\n\nProbable cause: The far end has a LOS, LOF, or AIS alarm on its receiving interface.\n\nPossible impact on the connections over this interface:\n- no calls are possible\n- loss of remote management access to other network elements in the RAN\n- loss of synchronization if the interface is used as a synchronization source\n\n		
Remedial action: 1. Check the intermediate transmission network for alarms indicating the root cause and follow the instructions for handling these alarms.\n\n2. Connect a loop cable and check that no alarms appear for this interface to check the transmit hardware.		

Table 40-78 FTM_RESET

Alarm	Attributes	Applicable major release
Name: FTM_RESET (11569) Type: communicationsAlarm Package: racfl.FTM_RESET Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_RESET Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_RESET\n\nThe transport part of the BTS has been reset at the date and time given in the notification.\n\n1. FSMr2 supports the following cause for the reset:\n\n'trs power-on reset': Cold start \n'trs watchdog reset': System overload\n'trs startup failure': Failure during startup \n'trs software failure': Software failure\n'trs management reset': Reset triggered by management interface\n'trs fallback': Fallback executed\n\nFSMr3/AirScale supports the following cause for the reset:\n\n'trs power-on reset': Cold start\n'trs watchdog reset': System overload\n'trs software failure': Software failure\n'trs management reset': Reset triggered by management interface\n'trs spurious reset': Reset reason detection failed\n\n2. The '$date' format is the local time stamp (GMT+/-xx:xx). For example: 2014-04-12 00:51:26 GMT+0530\n\nThe fault has no further consequences.\n\n		

Table 40-78 FTM_RESET (continued)

Alarm	Attributes	Applicable major release
Remedial action: No actions are required.		

Table 40-79 FTM_SECURITY_USER_ACCOUNT

Alarm	Attributes	Applicable major release
Name: FTM_SECURITY_USER_ACCOUNT (11570) Type: communicationsAlarm Package: racfl.FTM_SECURITY_USER_ACCOUNT Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_SECURITY_USER_ACCOUNT Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_SECURITY_USER_ACCOUNT\n\nA specific BTS local operator account has been locked.\nThe number of failed login attempts for a BTS local operator account has exceeded the threshold, and the account has been locked on the BTS. No further logins are permitted for this account until it is unlocked.\n\nNo further logins are permitted for that account until it is unlocked.\n\n		
Remedial action: Check the validity of the username and password of the account.		

Table 40-80 FTM_SFP

Alarm	Attributes	Applicable major release
Name: FTM_SFP (11571) Type: communicationsAlarm Package: racfl.FTM_SFP Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_SFP Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_SFP\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD/TDD:\nThe Small Form-Factor Pluggable (SFP) module detected in the interface connector does not comply with security requirements. It does not have a class 1 laser.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nThe Small Form-Factor Pluggable (SFP) module is not supported, not present, or could not be recognized.\nThe SFP module detected in the interface connector does not comply with the SFP module types supported by the BTS element. The SFP module type is checked to ensure that only laser class 1-compliant standard Ethernet SFP modules are used.\nThe SFP module was expected by the SW, but found missing.\nProbable causes:\n- No SFP module is inserted at the SFP-based Ethernet interface.\n- The interface contacts of the SFP module are corroded or dirty, preventing either read access to the SFP module at the time of reading compliance data from the SFP, or preventing detection of the module.\n- The SFP module type is not supported.\n\nThe fault is generated only when the interface is not configured as LMP (that is, generated only when the interface is configured as the primary BH port or when daisy chaining (enableLayer2Switching) is enabled).\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD/TDD:\nThe interface cannot be used for transmission.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nThe interface cannot be used for transmission. Conditionally, Bluetooth is enabled when the backhaul goes down.\nThe laser of the SFP module is not switched on, or no SFP module was detected at all.\nThe Ethernet Link is down.\nAn Ethernet Link cannot be successfully established.\nNo Ethernet data or clock information is exchanged between this interface.\n\nPossible impact on the connections over this interface:\n- Voice calls or data connections cannot be established.\n- Remote management connectivity cannot be established.\n- Loss of synchronization if the interface is used as a synchronization source.\n- Depending on use of the Ethernet interface, the above-described impact can occur for the local BTS and/or other BTS elements if they are chained through the Ethernet interface.\n\n		
Remedial action: Flexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD, AirScale BTS TDD:\nInsert a Small Form-Factor Pluggable (SFP) module with the correct laser type (class 1) to the Gigabit Ethernet interface of the unit.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\n1. Plug-out and plug-in the SFP module.\n2. Check for SFP validity (could be wrong type).\n3. Insert a compliant SFP module.		

Table 40-81 FTM_SFP_WARNING

Alarm	Attributes	Applicable major release
Name: FTM_SFP_WARNING (11572) Type: communicationsAlarm Package: racfl.FTM_SFP_WARNING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_SFP_WARNING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_SFP_WARNING\n\nThere is an issue with the SFP module used for backhaul. The fault is based on the SFP alarm and warning flags associated with temperature, supply voltage, TX bias current, and TX output power. Warning flags indicate conditions outside the normally-guaranteed bounds but not necessarily causes of immediate link failures while alarm flags can indicate pending, possible, or both pending and possible failure conditions. Certain warning flags might also be defined by the manufacturer as end-of-life indicators (such as for higher than expected bias currents in a constant power control loop). Warning flags are provided as an optional function with SFPs. The exact thresholds for the alarms and warnings are defined by the individual SFP manufacturer.\n\nThe backhaul via the SFP is in a degraded condition. The FZM BTS must be monitored for proper operation.\n\n		
Remedial action: Check the datasheet of the specific SFP used, whether the SFP warning flags are latching or non-latching. In case they are latching, reset the FZM or FZAP to determine whether the fault persists before taking further actions.\n1. Check whether the alarm is caused by exceeded temperature, internal supply voltage, or TX BIAS/TX output power.\n2. If exceeded temperature causes the alarm, investigate if the current operating conditions are outside the high or low temperature specifications for FZM or FZAP. If so, the warning clears when the temperature is within range. If it is inside the FZM- or FZAP-specified range, replace the SFP with an SFP supporting the full FZM or FZAP temperature range.\n3. If the internal supply voltage causes the alarm, check if the FZM or FZAP power input voltage is within the supported operating voltage range. If the FZM or FZAP power input is within the supported operating voltage range, then replace the SFP. Check the specifications of the SFP and whether it is interoperable with the FZM or FZAP. If the fault persists because of the internal supply voltage, replace the FZM or FZAP. If the FZM or FZAP power input voltage is outside the supported operating voltage range of the FZM or FZAP, correct the FZMor FZAP power input voltage.\n4. If the TX BIAS/TX output power causes the alarm, replace the SFP module.		

Table 40-82 FTM_SYNC_LOSS

Alarm	Attributes	Applicable major release
Name: FTM_SYNC_LOSS (11573) Type: communicationsAlarm Package: racfl.FTM_SYNC_LOSS Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_SYNC_LOSS Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_SYNC_LOSS\n\nPrimary and secondary timing sources are lost. The LTE is utilizing the Global Navigation Satellite System (GNSS) source (if available) or in synchronization hold-over mode.\n\nThe first and second synchronization sources from the configured priority list are unavailable. On failure, the LTE switches automatically to the next clock source in the priority list.\n\nProbable cause: The transmission links selected for clock source are faulty. The reason can be alarms on the interfaces (for example, LOS).\n\nPossible impact: The BTS is not synchronized to the network anymore.\n\n		
Remedial action: Use the BTS Site Manager to check which interfaces have been configured as synchronization sources.\n\n1. Check that the cables are connected to the correct connectors.\n2. Check whether the interface at the far end is switched on.\n3. Check whether there are active alarms at the far end. If there are, follow the instructions on handling those alarms.\n4. Connect a loop cable and check whether the alarm disappears to verify that the hardware of the interface unit works correctly.		

Table 40-83 FTM_TIMING_SOURCE_LOS

Alarm	Attributes	Applicable major release
Name: FTM_TIMING_SOURCE_LOS (11574) Type: communicationsAlarm Package: racfl.FTM_TIMING_SOURCE_LOS Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: FTM_TIMING_SOURCE_LOS Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: FTM_TIMING_SOURCE_LOS\n\nOne of the synchronization sources in the configured priority list is unavailable.\nThis can be the primary or the secondary clock source.\n\nIn the alarm: Protocol can be PDH, Timing over Packet (ToP), and Synchronuous ethernet.\n\nUnit Number is optional:\n- For PDH and Synchronous Ethernet, Unit number is 0 or 1.\n- It is not present for Timing Over Packet(TOP).\n\nThe interface value is optional:\n- For PDH, the value range depends on the hardware unit type: 1-16.\n- For Synchonuous Ethernet, the value range is 1-3.\n- It is not present for Timing over Packet.\n\nThe BTS may have to use a synchronization interface that has a lower clock\nquality: if the primary clock source has been lost, the BTS switches\nautomatically to the secondary clock source. If both the primary and the\nsecondary clock sources are lost, the BTS switches to the internal clock.\n\n		
Remedial action: Use BTS Site Manager to check which interfaces have been configured as\nsynchronization sources. For all interfaces, do as follows:\n\n1. Check that the cables are connected to the correct connectors.\n2. Check whether the interface at the far end is switched on.\n3. Check whether there are active alarms at the far end. If there are,\nfollow the instructions on handling those alarms.\n4. Connect a loop cable and check whether the alarm disappears to verify that the hardware of the interface unit works correctly.\n\nMonitor the quality of the received clock.		

Table 40-84 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • FL16A
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 40-85 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • FL16A
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		

Table 40-85 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 40-86 IPSEC_EMERGENCY_BYPASS_ACTIVE

Alarm	Attributes	Applicable major release
Name: IPSEC_EMERGENCY_BYPASS_ACTIVE (11575) Type: communicationsAlarm Package: racfl.IPSEC_EMERGENCY_BYPASS_ACTIVE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: IPSEC_EMERGENCY_BYPASS_ACTIVE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: IPSEC_EMERGENCY_BYPASS_ACTIVE\n\nThe BTS has entered the IPsec emergency bypass active state, where configured IPsec policies are ignored and the entire traffic is sent unprotected.\n\nConfigured IPsec policies are ignored, and the entire traffic is sent unprotected.\n\n		
Remedial action: Start IPsec emergency bypass by making the security gateway not reachable either\nby plugging out the cable or configuring wrong security gateway address.		

Table 40-87 IPSEC_EXPERT_MODE

Alarm	Attributes	Applicable major release
Name: IPSEC_EXPERT_MODE (11576) Type: communicationsAlarm Package: racfl.IPSEC_EXPERT_MODE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: IPSEC_EXPERT_MODE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: IPSEC_EXPERT_MODE\n\nBTS is in IPSec Expert Mode. This mode allows online tuning of IPSec related parameters for troubleshooting or workaround implementation via BTS Site Manager. It is meant for R&D troubleshooting only. When the fault is active, normal IPSec configuration changes are not recommended.\n\nIPSec expert settings can be configured on BTS via BTS Site Manager only if IPSec Expert Mode is activated.\n\n		
Remedial action: None.		

Table 40-88 IPsec_tunnel_switchover

Alarm	Attributes	Applicable major release
Name: IPsec_tunnel_switchover (11579) Type: communicationsAlarm Package: racfl.IPsec_tunnel_switchover Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: IPsec_tunnel_switchover Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: IPsec_tunnel_switchover\n\nThis alarm will be triggered when at least one primary IPSec tunnel fails, and BTS has switched over to a secondary IPSec tunnel.\nAs a result of failure in at least one primary IPSec tunnel, BTS has automatically switched over to a secondary IPSec tunnel terminating on secondary security gateway.\n\nBTS traffic has switched over from the primary IPSec tunnel to the secondary (backup) IPSec tunnel terminating on secondary security gateway.\n\nThe fault is cancelled when BTS has switched back all secondary tunnels to the primary IPSec tunnels due to automatic switchback or manual switchback request from the operator. This applies to the following state transitions:\n- Secondary_Active_Probing_Primary --> Primary_Active\n- Secondary_Active_No_Probing_Primary --> Primary_Active\n\nNote: The clear should also be sent when IPSec backup tunnel feature or IPSec feature is disabled, or BTS is rebooted.		
Remedial action: The operator can check the current remote tunnel endpoint parameter (ipSecBkupTunCurrRemoteEndpoint) on NetAct or BTS SM to verify the remote endpoint of a tunnel. The alarm will be cleared when the tunnel is switched back to the primary remote tunnel endpoint.		

Table 40-89 IPV6_DUPLICATE_ADDRESS_DETECTED

Alarm	Attributes	Applicable major release
Name: IPV6_DUPLICATE_ADDRESS_DETECTED (11577) Type: communicationsAlarm Package: racfl.IPV6_DUPLICATE_ADDRESS_DETECTED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: IPV6_DUPLICATE_ADDRESS_DETECTED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: IPV6_DUPLICATE_ADDRESS_DETECTED\n\nDuring the IP address configuration of the BTS, it tests the directly-attached network whether other, already configured BTSs, on the network already uses the same IP addresses on their network IP interfaces. The DAD detects those duplicated IP addresses and prohibits the operation of these IP addresses in the BTS. The warning shall contain the corresponding IP address. A separate reporting shall be indicated for each DAD event.\n\nThe remote peer to come online with the same IP address on the same subnet as\nlocal peer would just disable their network interface and give an error until\nthe situation is resolved by the administrator.\nThis allows the local peer to continue functioning without disruption, but completely breaks IP base communications for the connected network.\n\n		
Remedial action: 1.Check for duplicate IPv6 addresses configured in the BTS.\n2.Change or delete the identified duplicate IPv6 addresses.		

Table 40-90 IP_TRAFFIC_CAPTURE_ONGOING

Alarm	Attributes	Applicable major release
Name: IP_TRAFFIC_CAPTURE_ONGOING (11578) Type: communicationsAlarm Package: racfl.IP_TRAFFIC_CAPTURE_ONGOING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: IP_TRAFFIC_CAPTURE_ONGOING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-90 IP_TRAFFIC_CAPTURE_ONGOING (continued)

Alarm	Attributes	Applicable major release
Description: IP_TRAFFIC_CAPTURE_ONGOING\n\nThe base station is currently capturing an IP traffic towards a local port or into a file on the base station.\nIf the traffic capturing is happening towards a local port, a port and destination MAC address must be provided.\nPort values can be LMP or < HW MODULE NAME >-<PORT ID>.\n(For E.g: LMP or FSM-EIF1, FSM-EIF2 or FTIF-EIF1)\n\nNone\n\n		
Remedial action: An IP Traffic Capturing session is ongoing and a base station traffic is captured to a local Ethernet interface or into a file on the base station.		

Table 40-91 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • FL16A
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 40-92 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • FL16A
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 40-93 Link_OAM_critical_link_event__alarm

Alarm	Attributes	Applicable major release
Name: Link_OAM_critical_link_event__alarm (11581) Type: communicationsAlarm Package: racfl.Link_OAM_critical_link_event__alarm Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: Link OAM critical link event alarm Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: Link OAM critical link event alarm\n\nA Link OAM PDU containing a critical link event flag was received on the Ethernet interface. The alarm is raised with the first detection of the flag.\n\nThe following critical link events are possible:\n- Critical Event: either an Errored Symbol Period Event, an Errored Frame Event, an Errored Frame Period Event, or an Errored Frame Seconds Summary Event was detected.\n- Dying Gasp: either the local or the remote peer has a fatal error and is about to restart.\n- Link Fault: the local peer has detected a physical link fault in receiving direction, for example, a LOS.\n\nNote:\nIn case a received OAMPDU has more than one critical event flag set, the following shall be reported in the alarm:\nLink Fault bit set |Dying Gasp bit set|Critical Event bit set| Reported\n x x x Link Fault\n x x Link Fault\n x x Link Fault\n x x Dying Gasp\n\nAlways the latest received critical link event shall be reported.\n\nThe Ethernet interface is defective, or the remote peer is defective. Traffic might get lost.\n\nThe alarm shall be cleared only if OAMPDUs with cleared flag have been received for a configurable period of time (this assumes that the remote peer clears the flag when the error condition was solved).\nIt shall also be cleared when the Link OAM functionality on the interface is being reset.		
Remedial action: 1. Inspect details of the type of the critical event through online configuration management.\n2. Check the Link OAM state information of the interface.\n3. Check the cabling and network connections to the far end.\n4. Check the Ethernet interface configuration at the local and remote sides.\n5. Insert a Link OAM loopback.		

Table 40-94 Link_OAM_link_lost_alarm

Alarm	Attributes	Applicable major release
Name: Link_OAM_link_lost_alarm (11582) Type: communicationsAlarm Package: racfl.Link_OAM_link_lost_alarm Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: Link OAM link lost alarm Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: Link OAM link lost alarm\n\nOn an interface for which the Link OAM functionality was switched on, no Link OAM PDUs were received during the period specified in configuration parameter 'linkLostTime' (2-10 seconds, step 1 second).\n\nThe Ethernet interface might be out of order, or the remote peer might be out of order. Traffic might get lost.\n\nThe alarm is cleared automatically if link OAM PDUs are received continuously again during the same period specified in the parameter 'linkLostTime' (2-10 seconds, step 1 second).		
Remedial action: 1. Check the cabling and network connections to the far end.\n2. Check the Link OAM event information and the Link OAM state information.\n3. Check the Ethernet interface configuration at the local and remote sides.\n4. Insert a Link OAM loopback.		

Table 40-95 Link_OAM_loopback_alarm

Alarm	Attributes	Applicable major release
Name: Link_OAM_loopback_alarm (11583) Type: communicationsAlarm Package: racfl.Link_OAM_loopback_alarm Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: Link OAM loopback alarm Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-95 Link_OAM_loopback_alarm (continued)

Alarm	Attributes	Applicable major release
Description: Link OAM loopback alarm\n\nA loopback is requested for an Ethernet interface either locally at the BTS, or the Link OAM client of the BTS is set into loopback mode by the remote Link OAM peer.\n\nNormal traffic is interrupted. Only loopback OAM frames are transmitted and received over the interface. If the test frame generator is switched on, test frames are transmitted.\n\nFor a loopback inserted by the local peer, the alarm is cancelled automatically after the loopback has ended by expiration of configured loopback time. For a loopback inserted at the remote peer, the alarm is cancelled after detecting loopback end from the remote peer.		
Remedial action: None		

Table 40-96 LMP_CARRIER_DETECTED

Alarm	Attributes	Applicable major release
Name: LMP_CARRIER_DETECTED (11580) Type: communicationsAlarm Package: racfl.LMP_CARRIER_DETECTED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: LMP_CARRIER_DETECTED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: LMP_CARRIER_DETECTED\n\nThe Flexi Zone Micro BTS or Flexi Zone Access Point detects, using carrier state, that someone is locally connected to the small cell using LMP port.\n\nUpdate audit logs.\n\n		
Remedial action: 1. Determine if this event is expected: whether a qualified personnel is utilizing LMP ethernet port cable connection for diagnostic purposes. \n2. Otherwise, it shall be treated as a security warning.		

Table 40-97 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • FL16A
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 40-98 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • FL16A
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 40-99 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • FL16A
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 40-100 NEW_CONFIG_REJECTED

Alarm	Attributes	Applicable major release
Name: NEW_CONFIG_REJECTED (11584) Type: communicationsAlarm Package: racfl.NEW_CONFIG_REJECTED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: NEW_CONFIG_REJECTED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: NEW_CONFIG_REJECTED\n\nThis alarm is triggered once the new configuration file is rejected and the\nM-Plane connection is established with fallback configuration as a result\nof M-plane recovery action. It will be visible until next site reset.\n\nThe active base station configuration is not the same as requested in the configuration change.\n\n		
Remedial action: None		

Table 40-101 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • FL16A
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 40-102 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • FL16A
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 40-103 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • FL16A
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 40-104 NO_CERTIFICATE

Alarm	Attributes	Applicable major release
Name: NO_CERTIFICATE (11585) Type: communicationsAlarm Package: racfl.NO_CERTIFICATE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: NO_CERTIFICATE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: NO_CERTIFICATE\n\nA requested certificate could not be retrieved from the certificate authority (CA).\nA requested certificate could not be renewed from the certificate authority (CA).\n\nA requested certificate could not be retrieved as the number of certificates received from repository server (RA) or certificate authority (CA) are more than expected.\n\nA requested certificate could not be stored in the remaining storage available on the BTS. Operator cleanup (e.g. via site manager or NetAct) of old, unused trust chains may be required.\n\nThe requested service is not available.\n\n		
Remedial action: Provide the certificate.		

Table 40-105 NTP_SERVER_UNREACHABLE

Alarm	Attributes	Applicable major release
Name: NTP_SERVER_UNREACHABLE (11586) Type: communicationsAlarm Package: racfl.NTP_SERVER_UNREACHABLE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: NTP_SERVER_UNREACHABLE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A

Table 40-105 NTP_SERVER_UNREACHABLE (continued)

Alarm	Attributes	Applicable major release
Description: NTP_SERVER_UNREACHABLE\n\nFlexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD/TDD, Flexi Zone Micro FDD, Flexi Zone Micro TDD:\nA BTS reports this alarm for each instance of the configured NTP server if that\nparticular NTP server is not accessible or cannot be used after waiting for\na threshold timeout defined by the INTP::ntpAlarmThreshold configuration parameter in PDDB.\n\nThe raised alarm displays the IP address of the NTP server that is not reachable\nin the additional information field 'alarmNotif::argumentInfo'.\n\nNote : For each NTP server instance, timers are started separately and a separate\nalarm is raised. This threshold time is not used to clear the alarm.\n\nFlexi Zone:\nFlexi Zone Access Point reports this alarm for each instance of the configured\nNTP server if that particular NTP server is not accessible or cannot be used\nafter waiting for a threshold time-out defined by the configuration parameter\nINTP::ntpAlarmThreshold in PDDB.\n\nThe raised alarm displays the IP address of the NTP server that is not reachable\nin the additional information field 'alarmNotif::argumentInfo'.\n\nNote : For each NTS server instance, timers are started separately and a separate\nalarm is raised. This threshold time is not used to clear the alarm.\n\nThe BTS might lose time synchronization if there are problems with multiple NTP servers, or the BTS will have no time synchronization at all if all NTP servers are down.\n\nFlexi Zone:\nFlexi Zone Access Point might lose time synchronization if there are problems with multiple NTP servers, or the BTS will have no time synchronization at all if all NTP servers are down.\n\n		
Remedial action: 1. Check the connectivity to the NTP server.\n2. Check the NTP server configuration at the BTS.\n3. Check the configured threshold value for the NTP server.		

Table 40-106 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • FL16A
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 40-107 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • FL16A
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		

Table 40-107 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 40-108 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • FL16A
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 40-109 PLR_THRESHOLD_CROSSED

Alarm	Attributes	Applicable major release
Name: PLR_THRESHOLD_CROSSED (11587) Type: communicationsAlarm Package: racfl.PLR_THRESHOLD_CROSSED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: PLR_THRESHOLD_CROSSED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: PLR_THRESHOLD_CROSSED\n\nThe alarm is raised if the packet loss ratio equals or exceeds the configured\ nthreshold value during the current observation interval of 15 minutes.\n\nThis alarm is an indication that the backhaul capacity for traffic with same\nprofile as this TWAMP session (DSCP value, packet size), may be much too small,\nbecause some of the measurement packets seem to have been thrown away.\n\nThe TWAMP measurement packets are lost because of degraded traffic throughput.\n\n		
Remedial action: 1. Check the backhaul usage and if other applications with the same or higher\nPHB may compete against this TWAMP session about the capacity. An increase in\nthe priority of TWAMP session or of the backhaul capacity may clear the alarm.\n\n2. Check if destination is unreachable by IP connectivity test. Send an ICMP\necho request (ping) to the UDP port of the TWAMP reflector at the destination\nIP.If ICMP echo reply indicates that the destination is unreachable but you\nhave access to TWAMP reflector, you can check its status. If the status is disabled\nor down try to activate it again and check if alarm disappears.\n\n3. Check configured PLR threshold. Setting PLR to 0% should be avoided, because\nevery lost measurement packet will trigger the alarm and it cannot be cleared\nagain (PLR>="0)."		

Table 40-110 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • FL16A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 40-111 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • FL16A
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 40-112 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • FL16A
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 40-113 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • FL16A
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 40-114 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • FL16A
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 40-115 RTT_THRESHOLD_CROSSED

Alarm	Attributes	Applicable major release
Name: RTT_THRESHOLD_CROSSED (11588) Type: communicationsAlarm Package: racfl.RTT_THRESHOLD_CROSSED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: RTT_THRESHOLD_CROSSED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: RTT_THRESHOLD_CROSSED\n\nThe RTT threshold alarm is sent in case the average value of the RTT exceeds or equals the configured threshold for a 1-min period.\n\nThis alarm is an indication that the backhaul capacity for traffic with the\nsame profile as this TWAMP session (DSCP value, packet size) may be too small,\nbecause the measurement packets are scheduled later than before.\n\n		

Table 40-115 RTT_THRESHOLD_CROSSED (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Check the backhaul usage and if other applications with the same or higher\nPHB may compete against this TWAMP session about the capacity. An increase in\nthe priority of TWAMP session or of the backhaul capacity may clear the alarm.\n\n2. Check the last measured RTT values of this TWAMP session and verify that\nthe configured RTT threshold value is not too close to average measured RTT\nvalues, so that this alarm could be result of sporadic mis-measurement.		

Table 40-116 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • FL16A
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 40-117 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • FL16A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 40-118 SFP_HW_Failure

Alarm	Attributes	Applicable major release
Name: SFP_HW_Failure (11589) Type: communicationsAlarm Package: racfl.SFP_HW_Failure Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: SFP HW Failure Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: SFP HW Failure\n\nA malfunctioning of the SFP transceiver was detected. \nThe SFP has reported a transmission fault condition and has disabled the laser transmitter.\n\nThe SFP is not operational.\n\nThe BTS checks if the HW unit is working correctly.		
Remedial action: Replace the faulty SFP. Note that only the SFP might be faulty, not necessarily the entire hardware unit.		

Table 40-119 SSH_ENABLED

Alarm	Attributes	Applicable major release
Name: SSH_ENABLED (11590) Type: communicationsAlarm Package: racfl.SSH_ENABLED Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: SSH_ENABLED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: SSH_ENABLED\n\nThe Flexi Zone Micro BTS or Flexi Zone Access Point detects that the SSH access to the site is enabled.\n\nNote: The SSH access to the site is disabled by default. To mitigate the risk in field scenarios, SSH should only be enabled for limited periods time on an as-needed basis.\n\nUpdate audit logs.\n\n		
Remedial action: 1. Determine if this event is expected.\nNote: The SSH access to the site is disabled by the default. SHH should only be enabled for limited periods time on an as-needed basis.		

Table 40-120 SSM_POORQUALITY

Alarm	Attributes	Applicable major release
Name: SSM_POORQUALITY (11591) Type: communicationsAlarm Package: racfl.SSM_POORQUALITY Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: SSM_POORQUALITY Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: SSM_POORQUALITY\n\nThis alarm is raised when the received SSM indicates lower clock quality (for example, 'do not use' or 'EEC') than required.\n\nNote: The interface numbering shall be similar to ETHLK.\nE.g: DN:SYNC-1/STPG-1/STPU-1-4 for unit 1,interface 4.\n\nFlexi Zone Micro FDD, Flexi Zone Micro TDD:\nSyncE is no longer a working synchronization source.\n\nThe alarm is cleared if one SSM is received again showing sufficient quality level.		
Remedial action: Flexi Zone Micro FDD, AirScale BTS FDD/TDD, Flexi Zone Micro TDD, Flexi Zone:\n1. Confirm that SyncE is desired as a synchronization source.\n2. Confirm that eNB configuration settings for ssmEnabled are correct.\n3. Troubleshoot with Backhaul provider on the reason SSM errors.		

Table 40-121 SSM_TIMEOUT

Alarm	Attributes	Applicable major release
Name: SSM_TIMEOUT (11592) Type: communicationsAlarm Package: racfl.SSM_TIMEOUT Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: SSM_TIMEOUT Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: SSM_TIMEOUT\n\nThis alarm is raised if the incoming SSM is not received for a certain time period (configured through the parameter 'ssmTimeout').\n\nNote: The interface numbering is similar to ETHLK.\nExample: DN:SYNC-1/STPG-1/STPU-1-4 for unit 1, interface 4\n\nSyncE is no longer a working synchronization source.\n\n		
Remedial action: 1. Confirm that SyncE is desired as a synchronization source.\n2. Confirm that configuration settings for ssmEnabled are correct.\n3. Troubleshoot with backhaul provider about the reason for SSM errors.		

Table 40-122 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • FL16A
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 40-123 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • FL16A
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 40-124 TOP_MASTER_UNUSABLE

Alarm	Attributes	Applicable major release
Name: TOP_MASTER_UNUSABLE (11593) Type: communicationsAlarm Package: racfl.TOP_MASTER_UNUSABLE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: TOP_MASTER_UNUSABLE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: TOP_MASTER_UNUSABLE\n\nThe reference clock monitoring has detected a loss of ToP reference clock signal received from the master clock behind $IP:\n- The eNB does not receive a reply from ToP Master within a certain time (5 sec) upon sending a sync request message.\n- The eNB receives from ToP Master granted message rates (sync message rate, delay message rate), that do not match the requested rate by the eNB.\n\nThere might be another synchronization source available at eNB. In that case, the BTS switches automatically to the other clock source.\n\nIf no other synchronization source is available at eNB, it runs in hold-over mode. \n\nPlease refer to status of '3080: EFaultId_BtsReferenceClockMissing'.\n\n		
Remedial action: 1. Check the cable connectivity.\n2. Check the TOP configuration.		

Table 40-125 TRANSPORT_MODULE_MISSING

Alarm	Attributes	Applicable major release
Name: TRANSPORT_MODULE_MISSING (11594) Type: communicationsAlarm Package: racfl.TRANSPORT_MODULE_MISSING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: TRANSPORT_MODULE_MISSING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: TRANSPORT_MODULE_MISSING\n\nA unit is missing. The slot has been configured to hold a unit, but the plug-in\nunit is not physically present in the slot.\n\nProbable causes:\n\n- The unit has been configured but not detected.\n- The unit is broken and therefore not detected.\n- The unit has been configured but some other unit is detected.\n\nNOTE: The unit variable should be replaced by appropriate HW names configured (unitTypeConfigured) during runtime reporting.\n\nPossible impacts:\n- No calls are possible for the connections over this unit.\n- Remote management access to other network elements in the RAN is lost.\n\n		
Remedial action: Replacing a faulty hardware:\n1. Plug in again the expected transport unit that is referenced in the alarm text.\n2. In case there is a unit present in the slot, remove it from the slot\nand plug it back in. If the unit is still not recognized and the alarm\nremains, replace the faulty unit with a new one. \n\nDecommissioning a previously commissioned hardware:\n1. Recommission to remove the hardware unit referenced in the alarm text.\n\nNOTE: Before recommissioning, the hardware unit must not be present in the slot.		

Table 40-126 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • FL16A
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		

Table 40-126 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 40-127 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • FL16A
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 40-128 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw.TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • FL16A
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 40-129 TRUST_ANCHOR_EXPIRING

Alarm	Attributes	Applicable major release
Name: TRUST_ANCHOR_EXPIRING (11595) Type: communicationsAlarm Package: racfl.TRUST_ANCHOR_EXPIRING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: TRUST_ANCHOR_EXPIRING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: TRUST_ANCHOR_EXPIRING\n\nThe network element stores trust anchors for its own trust chain and for peers. When its own or any trust anchors are about to expire or are expired, this alarm is sent.\n\nNo immediate effect. If at all certificate expires without any action from operator due to this fault, secure communication to remote peers may fail.\n\n		
Remedial action: Update the trust anchors.		

Table 40-130 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • FL16A
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		

Table 40-130 UnidentifiedNode (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 40-131 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • FL16A
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 40-132 UNSUPPORTED_HW_DEVICE

Alarm	Attributes	Applicable major release
Name: UNSUPPORTED_HW_DEVICE (11597) Type: communicationsAlarm Package: racfl.UNSUPPORTED_HW_DEVICE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: UNSUPPORTED_HW_DEVICE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: UNSUPPORTED_HW_DEVICE\n\nThe SW does not support the detected HW unit type.\n\nProbable causes:\n\n- The SW version of the system module is too old.\n- The supported HW variant is not present in the system module.\n\nThe possible impact is that no calls are possible for the connections over this unit.\n\n		
Remedial action: SW upgrading: Upgrade the FSM SW release to the latest version that includes the support for the new external transport device variant.\n\nUnit variant replacement: Replace the unsupported device variant to another one that supports the currently running SW release.		

Table 40-133 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • FL16A

Table 40-133 UpgradedBuildVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 40-134 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • FL16A
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 40-135 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • FL16A
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 40-136 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • FL16A
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 40-137 VENDOR_CERTIFICATE_EXPIRING

Alarm	Attributes	Applicable major release
Name: VENDOR_CERTIFICATE_EXPIRING (11598) Type: communicationsAlarm Package: racfl.VENDOR_CERTIFICATE_EXPIRING Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: VENDOR_CERTIFICATE_EXPIRING Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: VENDOR_CERTIFICATE_EXPIRING\n\nThe BTS raises this alarm when the vendor BTS certificate is about to expire.\n\nThe period of advance notification is configurable, as well as the CA certificate expiry.\n\n1 day ... 4999 days with default 90 days\n\nNote: For Flexi Zone Controller, the period of advance notification is a non-configurable 90 days.\n\nAs long as BTS operator certificate is available and active on BTS, there is no impact. However, if BTS is reset to factory default, since vendor certificate is expired, the BTS may fail to derive a new BTS operator certificate.\n\n		
Remedial action: Flexi BTS FDD, Flexi BTS TDD, AirScale BTS FDD/TDD, Flexi Zone Micro FDD, Flexi Zone Micro TDD, Flexi Zone Access Point, Flexi Zone Controller:\nCheck the vendor BTS certificate expiry date. \nReplace the expired vendor BTS certificate if possible (for example, an older BTS like FSMr2).\nOtherwise, contact Nokia to investigate the need for hardware replacement or return to resolve the possible end-of-life indication implied by the expired Nokia vendor certificate.\n\nFor most BTS types (including at least FSMr3, Airscale, Flexi Zone Controller, FZAP, and Flexi Micro/Pico), a new vendor certificate can only be installed in the Nokia factory.		

Table 40-138 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • FL16A
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		

Table 40-138 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 40-139 WIFI_CARD_INVALID_TYPE

Alarm	Attributes	Applicable major release
Name: WIFI_CARD_INVALID_TYPE (11599) Type: communicationsAlarm Package: racfl.WIFI_CARD_INVALID_TYPE Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: WIFI_CARD_INVALID_TYPE Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: WIFI_CARD_INVALID_TYPE\n\nThe internal Wi-Fi module type is invalid.\n\nThe internal Wi-Fi module might not be operational.\n\n		
Remedial action: 1. Check the release notes of the downloaded BTS software if any known Wi-Fi module issues are reported.\n2. Replace the Flexi Zone Micro BTS.		

Table 40-140 WIFI_CARD_NOT_PRESENT

Alarm	Attributes	Applicable major release
Name: WIFI_CARD_NOT_PRESENT (11600) Type: communicationsAlarm Package: racfl.WIFI_CARD_NOT_PRESENT Raised on class: racfl.MRBTS	Severity: indeterminate Specific problem: WIFI_CARD_NOT_PRESENT Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • FL16A
Description: WIFI_CARD_NOT_PRESENT\n\nThe internal Wi-Fi module is not present.\n\nThe internal Wi-Fi module might be not operational.\n\n		
Remedial action: 1. Check the release notes of the downloaded BTS software if any known Wi-Fi module issues are reported.\n2. Replace the Flexi Zone BTS.		

Table 40-141 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • FL16A
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		

Table 40-141 WrongCpaaSoftwareVersion (continued)

Alarm	Attributes	Applicable major release
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

41 LTE OMS

41.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 41-1 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • LOMS16A
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 41-2 ACTIVE_ALARM_OVERFLOW

Alarm	Attributes	Applicable major release
Name: ACTIVE_ALARM_OVERFLOW (11601) Type: qualityOfServiceAlarm Package: racloms.ACTIVE_ALARM_OVERFLOW Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ACTIVE ALARM OVERFLOW Implicitly cleared: true Default probable cause: RESOURCE_AT_OR_NEARING_CAPACITY	Release: • LOMS16A
Description: ACTIVE ALARM OVERFLOW\n\nThe maximum limit for the amount of active alarms has been reached in AlarmSystem database.\n\nWhile the node has the maximum amount of active alarms, alarms originated from controller are rejected, alarms originated from OMS are cached in file. Clearing of the alarms is anyhow possible.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check active alarms on the overflowing node with alarm management application and correct them according to their instructions. If this is not possible or does not cause this alarm to be removed, fill in a Problem Report and send it to your local Nokia representative.		

Table 41-3 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LOMS16A
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 41-4 ALARM_FROM_NE_CORRUPTED

Alarm	Attributes	Applicable major release
Name: ALARM_FROM_NE_CORRUPTED (11602) Type: qualityOfServiceAlarm Package: racloms.ALARM_FROM_NE_CORRUPTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM FROM NE CORRUPTED Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: ALARM FROM NE CORRUPTED\n\nOMS could not decode alarm message from NE.\n\nOMS does not have working alarm interface to that NE.\n\nDo not clear the alarm. OMS will clear the alarm automatically.		
Remedial action: Possible reason is false BTSOM interface version. Contact Nokia representative.		

Table 41-5 ALARM_LOG_FILE_INACCESSIBLE

Alarm	Attributes	Applicable major release
Name: ALARM_LOG_FILE_INACCESSIBLE (11603) Type: processingErrorAlarm Package: racloms.ALARM_LOG_FILE_ INACCESSIBLE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM LOG FILE INACCESSIBLE Implicitly cleared: true Default probable cause: FILE_ERROR	Release: • LOMS16A
Description: ALARM LOG FILE INACCESSIBLE\n\nAlarm processor cannot open or read the alarm log file.\n\nAlarm notifications recorded in the alarm log file cannot reach the alarm system, and as a result the control for the alarm situation in the network element is lost.\n\nThe alarm is cleared automatically by the alarm system when access to the alarm log file is restored.		

Table 41-5 ALARM_LOG_FILE_INACCESSIBLE (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Check with the parameter management application that the alarm log file name in the alarm processor configuration in LDAP (fsParameterId="fsLogFileName, fsAlarmProcessorConfigurationId=Default, fsAlarmProcessorId= AlarmProcessor1, fsFragmentId= AlarmProcessors, fsFragmentId=AlarmMgmt, fsClusterId=ClusterRoot) is the same as the name specified in the Management Object Model in the SS_MOMfsAlarm document. \n2. If the value in LDAP is different, then modify the LDAP value and restart alarm processor with the following command:\nfshascli -r /<Node>/FSAlarmSystemServer/AlarmProcessor\ nwhere <Node> is the name of the node where alarm processor is deployed.\n3. If the values are the same, then fill in a problem report with the alarm data and send it to your Nokia representative."		

Table 41-6 ALARM_OVERFLOW_CACHE_FILE_INACCESSIBLE

Alarm	Attributes	Applicable major release
Name: ALARM_OVERFLOW_CACHE_FILE_ INACCESSIBLE (11604) Type: processingErrorAlarm Package: racloms.ALARM_OVERFLOW_CACHE_ FILE_INACCESSIBLE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM OVERFLOW CACHE FILE INACCESSIBLE Implicitly cleared: true Default probable cause: FILE_ERROR	Release: • LOMS16A
Description: ALARM OVERFLOW CACHE FILE INACCESSIBLE\n\nAlarm processor cannot open or read the alarm overflow cache file.\n\nIt's impossible to cache incoming alarm notifications if the Alarm System will be in overload state.\n\nDo not clear the alarm. The system will automatically clear the alarm.		
Remedial action: 1. Check if the name of the overflow cache alarm log file that is defined by the parameter fsOverflowAlarmCacheFile in the alarm processor configuration in Configuration Directory points out to the existing file name (excluding number suffix). \nldapsearch -LLL -H ldap://Directory:389 -x -b "fsClusterId="ClusterRoot" "(objectclass=FSAlarmProcessorConfiguration)"\n\n2. If these files (with number suffixes 0,1, etc..) don't exist, it's possible to leave existing defined filename or change it in the Configuration Directory (LDAP) using the following SCLI commands:\nldapmodify -x -y /opt/Nokia_BP/etc/ldapfiles/fssecldap.ldaproot -D uid=fsLDAPRoot,ou=People,fsFragmentId=Security,fsClusterId=ClusterRoot<<EOF\ndn: fsAlarmProcessorConfigurationId=Default, fsAlarmProcessorId=AlarmProcessor1,fsFragmentId=AlarmProcessors,fsFragmentId=AlarmMgmt,fsClusterId= ClusterRoot\nfsOverflowAlarmCacheFile: <correct_value> EOF\n\nThen restart the Alarm System using the following SCLI command:\nfshascli -r /AlarmSystem\n\nAfter the Alarm System restarts, files should be recreated anew in the given location.\n\n3. If alarm is still active after the Alarm System restart, prepare a problem report with the alarm data, and send it to your Nokia representative."		

Table 41-7 ALARM_PROCESSOR_CONFIGURATION_IS_OUT_OF_ORDER

Alarm	Attributes	Applicable major release
Name: ALARM_PROCESSOR_CONFIGURATION_ IS_OUT_OF_ORDER (11605) Type: processingErrorAlarm Package: racloms.ALARM_PROCESSOR_ CONFIGURATION_IS_OUT_OF_ORDER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM PROCESSOR CONFIGURATION IS OUT OF ORDER Implicitly cleared: true Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A
Description: ALARM PROCESSOR CONFIGURATION IS OUT OF ORDER\n\nThe configuration of alarm processor contains an invalid attribute value or an attribute is missing.\n\nThe system ignores the invalid value and uses a default value.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-7 ALARM_PROCESSOR_CONFIGURATION_IS_OUT_OF_ORDER (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Use the parameter management application to correct the invalid value of the attribute. The distinguished name of the attribute - identifying its location in the LDAP - can be found in the 'Managed Object Id' field of the alarm. \n2. Restart alarm processor with the following command:\nfshascli -r /<Node>/FSAlarmSystemServer/AlarmProcessor\nwhere <Node> is the name of the node where alarm processor is deployed.\nThe default values of the alarm processor attributes used when correcting the situation are listed below:\nAttribute Default value\nfsNumProcessors: 5\nfsHasSimpleAware: true\nfsLogFileName: /var/log/master-alarms\ nfsLogParserSleepTime: 1\nfsAlarmNotificationCollectorSleepTime:\n 1\nfsParameterNotificationProcessorSleepTime:\n 15\nfsAlarmHistoryProcessorSleepTime:\n 60\nfsAlarmHistorySize: 1000000\nfsBatchSize: 120\nfsHeartbeatInterval: 300\ nfsAlarm70247raise: true\nfsSeverityChangeReRaise: false\nfsNotificationBatchSize: 20\nfsStrictAlarmTimeOrder: false\ nfsAllowedMCACAlarms: true\nfsDatSupport: true\nfsAutoAckedDAT: true\nfsTimeBasedAlarmHistorySize: false\ nfsDeletedAlarmHistorySize: 4000\nfsStoredAlarmNotificationsPerSecond: \n 0\nfsZeroTTLforWarnings: false\ nfsOriginalTimeAsAlarmTimeForExternals: \n rnw="0 crnc=0 fp=0\nfsUseTimeParamsForExternals: rnw=0 crnc=0 fp=0\ nfsRaise70280insteadOf70005forUnknownSP: \n true\nfsAlarmIndicationPreventionList:\n 70246=5\nfsExternalFlowControlValid: rnw=1 crnc=1 fp=1\nfsSendParameterChangeNotification: \n false\nfsSendRuleChangeNotification: false"		

Table 41-8 ALARM_SYSTEM_HEARTBEAT

Alarm	Attributes	Applicable major release
Name: ALARM_SYSTEM_HEARTBEAT (11606) Type: processingErrorAlarm Package: racloms.ALARM_SYSTEM_HEARTBEAT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM SYSTEM HEARTBEAT Implicitly cleared: true Default probable cause: TIMEOUT_EXPIRED	Release: • LOMS16A
Description: ALARM SYSTEM HEARTBEAT\n\nThis is an informative alarm, which indicates that the alarm system itself is in operational state.\n\nThe alarm system is continuously (after each expiration of a heartbeat interval) raising or clearing this alarm, which means that the state of this alarm is constantly changing in a loop (new alarm -> cleared alarm -> new alarm -> cleared alarm -> new alarm -> ...) and the alarm time is updated by the time of the last raise/clear operation. If the refreshing of the alarm does not occur, it signals that the alarm system is faulty.\nNote that there is a delay before the raise/clear operation becomes visible in the alarm monitoring tool. If the system is under heavy load it might take even longer for the operation to be visible in the alarm monitoring tool.\n\nThe alarm system clears the alarm when the heartbeat interval expires.		
Remedial action: 1. If the used alarm monitor tool does not support an automatic alert in situations where the alarm system heartbeating is not functioning, check occasionally that the heartbeating functions properly. The time of the alarm and the value of the heartbeat interval (specified in the 'Application Additional Info' field) should be used in analysing the situation. \n2. Perform such checking also when the system does not generate any alarm events for a long time.\n3. If the checking shows that the alarm time is not continuously refreshed, restart the alarm processor with the following command:\nfshascli -r /<Node>/FSAlarmSystemServer/ AlarmProcessor\nwhere <Node> is the name of the node where the alarm processor is deployed.\n4. If restarting the alarm processor does not help, also restart the alarm system database with the following command:\nfshascli -r /AlarmDB		

Table 41-9 ALARM_SYSTEM_HEARTBEATING_SWITCHED_OFF

Alarm	Attributes	Applicable major release
Name: ALARM_SYSTEM_HEARTBEATING_ SWITCHED_OFF (11607) Type: processingErrorAlarm Package: racloms.ALARM_SYSTEM_ HEARTBEATING_SWITCHED_OFF Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM SYSTEM HEARTBEATING SWITCHED OFF Implicitly cleared: true Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A

Table 41-9 ALARM_SYSTEM_HEARTBEATING_SWITCHED_OFF (continued)

Alarm	Attributes	Applicable major release
Description: ALARM SYSTEM HEARTBEATING SWITCHED OFF\n\nThe alarm system heartbeating is switched off, which means that the alarm system does not raise or clear its heartbeat alarms.\n\nThe alarm system heartbeating is the simplest and most efficient way for the operator to monitor that the alarm system itself is healthy. If the system is in a switched off state, the operator cannot detect if the alarm system becomes faulty. This is why it is strongly recommended that you have the alarm system heartbeating always switched on. Nevertheless the alarm system heartbeating can be switched off if an alternative heartbeating exists. In the alarm system configuration, by setting the value of the fsAlarm70247raise configuration parameter to false, raising the 70247 alarm will be disabled.\n\nThe alarm system clears the alarm automatically after restart if the alarm system heartbeating is set as switched on in the configuration.		
Remedial action: 1. Use the parameter management application to set a non-zero (0 means that heartbeating is switched off) heartbeat interval in seconds for the fsParameterId=" fsHeartbeatInterval, fsAlarmProcessorConfigurationId=Default, fsAlarmProcessorId=AlarmProcessor1, fsFragmentId= AlarmProcessors, fsFragmentId=AlarmMgmt, fsClusterId=ClusterRoot attribute in the alarm system LDAP configuration. \n2. Use the parameter management application to set the value of the fsParameterId=fsAlarm70247raise, fsAlarmProcessorConfigurationId=Default, fsAlarmProcessorId=AlarmProcessor1, fsFragmentId= AlarmProcessors, fsFragmentId=AlarmMgmt, fsClusterId=ClusterRoot attribute to false in the alarm system LDAP configuration for the case when the alarm system heartbeating is desired to be switched off.\n3.Restart alarm processor with the following command:\nfshascli -r /<Node>/FSAlarmSystemServer/AlarmProcessor\nwhere <Node> is the name of the node where alarm processor is deployed."		

Table 41-10 ALARM_TYPE_PARAMETER_HAS_BEEN_MODIFIED

Alarm	Attributes	Applicable major release
Name: ALARM_TYPE_PARAMETER_HAS_BEEN_MODIFIED (11608) Type: processingErrorAlarm Package: racloms.ALARM_TYPE_PARAMETER_HAS_BEEN_MODIFIED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ALARM TYPE PARAMETER HAS BEEN MODIFIED Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: ALARM TYPE PARAMETER HAS BEEN MODIFIED\n\nSome parameters for alarm type have been modified.\n\nThe changed parameters affect the processing of the alarms, that belong to the alarm type in question.\n\nThe system clears the alarm automatically after its time to live\nhas expired.		
Remedial action: This is an informative alarm which indicates that an operator has modified some parameters for an alarm type. The alarm doesn't require any action.		

Table 41-11 APPLICATION_CONFIGURATION_IS_OUT_OF_ORDER

Alarm	Attributes	Applicable major release
Name: APPLICATION_CONFIGURATION_IS_OUT_OF_ORDER (11609) Type: processingErrorAlarm Package: racloms.APPLICATION_CONFIGURATION_IS_OUT_OF_ORDER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: APPLICATION CONFIGURATION IS OUT OF ORDER Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A

Table 41-11 APPLICATION_CONFIGURATION_IS_OUT_OF_ORDER (continued)

Alarm	Attributes	Applicable major release
Description: APPLICATION CONFIGURATION IS OUT OF ORDER\n\nThe configuration of an application contains an invalid attribute value or an attribute is missing.\n\nDepending on the alarm severity, application's start-up or run-time session can fail (CRITICAL severity), application can partially loose functionality (MAJOR severity) or ignore the invalid configuration and use default or the closest acceptable value(s) (MINOR severity).\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Observe the application in question by checking the 'Application Id' field of the alarm.\n\n2. Lock the application in the case of a CRITICAL severity alarm to prevent its infinite restart using command:\nfshascli -l <Application Id>\n\n3. Observe the invalid or missing attribute by checking the 'Identifying Additional Info' field of the alarm.\n\n4. Observe the configuration location by checking the 'Managed Object' field (which contains, for example, a branch for the LDAP-based configuration or a path for the file-based one).\n\n5. Add or correct the invalid attribute mentioned in the 'Identifying Additional Info' field. Follow the guidelines in the customer documentation for the application using the appropriate tool (for example, a text editor for the file-based configuration).\n\n6. Unlock (if the second step was used) or restart the application with commands:\n- unlock:\nfshascli -u <Application Id>\n- restart\nfshascli -r <Application Id>		

Table 41-12 AUTHENTICATION_FAILURE_IN_ETHERNET_DEVICE

Alarm	Attributes	Applicable major release
Name: AUTHENTICATION_FAILURE_IN_ ETHERNET_DEVICE (11610) Type: equipmentAlarm Package: racloms.AUTHENTICATION_FAILURE_IN_ ETHERNET_DEVICE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: AUTHENTICATION FAILURE IN ETHERNET DEVICE Implicitly cleared: false Default probable cause: PROTECTION_PATH_ FAILURE	Release: • LOMS16A
Description: AUTHENTICATION FAILURE IN ETHERNET DEVICE\n\nThe alarm is triggered by the authenticationFailure SNMP trap. The SNMP agents running in the Ethernet switches (switch blades or modules) generate the trap, if they receive SNMP requests that are not properly authenticated. SNMPv1 and SNMPv2c use community names to provide security, authentication, and access control:\n1. Each community name has an associated access mode (either read-only or read-write).\n2. Each community name has an associated IPv4 subnet/mask.\n3. Each community name may be enabled or disabled.\nThe SNMP agent rejects and discards any SNMP requests that do not contain a community name that matches one of the configured community names, or which do not contain an IPv4 source address that is allowed by the corresponding community name's IPv4 address and IPv4 mask. More specifically, the following authentication failures are detected for SNMP requests:\n1. Each getRequest, getNextRequest, or getBulkRequest that does not include one of the enabled read-only or read-write community names.\n2. Each setRequest that does not include one of the enabled read-write community names.\n3. Each SNMP message sent from an invalid IPv4 subnet.\n\nThe alarm may indicate that an SNMP tool used for sending SNMP requests to the SNMP agent, or the SNMP agent, is configured incorrectly. The alarm may also indicate malicious activity, meaning that an unauthorised user is trying to obtain information by sending SNMP requests.\n\nClear the alarm with the alarm management application after correcting the fault.		
Remedial action: Login to the switch by ssh and start the CLI (command line interface) of the switch by entering swc. Use the following CLI commands for verifying and modifying the configured SNMP community names:\nshow snmpcommunity\nconfig snmpcommunity accessmode <ro/rw> <community name>\nconfig snmpcommunity create <community name>\nconfig snmpcommunity delete <community name>\nconfig snmpcommunity ipaddr <IP Addr of switch> <community name>\nconfig snmpcommunity ipmask <ipmask> <community name>\nconfig snmpcommunity mode <enable/disable> <community name>\nconfig snmptrap create <Name> <IP Addr of SNMPMediator>		

Table 41-13 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LOMS16A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 41-14 BACKEND_DATABASE_REQUIRED_BY_CORBA_NAMING_SERVICE_IS_UNAVAILABLE

Alarm	Attributes	Applicable major release
Name: BACKEND_DATABASE_REQUIRED_BY_CORBA_NAMING_SERVICE_IS_UNAVAILABLE (11611) Type: processingErrorAlarm Package: racloms.BACKEND_DATABASE_REQUIRED_BY_CORBA_NAMING_SERVICE_IS_UNAVAILABLE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BACKEND DATABASE REQUIRED BY CORBA NAMING SERVICE IS UNAVAILABLE Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_UNAVAILABLE	Release: • LOMS16A
Description: BACKEND DATABASE REQUIRED BY CORBA NAMING SERVICE IS UNAVAILABLE\n\nThe MySQL database instance DB_CosNaming, used by the private CORBA naming service (NaS) instance, cannot be contacted by the NaS wrapper. Note that the recovery group that owns the backend database is NamingServiceDB and CORBA NaS instances belong to recovery group PrivateCosNaming.\n\nThe CORBA NaS is not able to store data in the database. Therefore the CORBA NaS is not functional.\n\nWhen CORBA NaS detects that MySQL database instance DB_CosNaming is available it re-establishes the connection to the database and clears the alarm.		
Remedial action: Check that the error situation still exists:\n /opt/Nokia/SS_Naming/bin/ns_listall\n /opt/Nokia/SS_Naming/bin/ns_listall public\nThese commands should list the content of the private and the public naming graphs when the NaS is working correctly. \nIf these commands throw exceptions, the NaS is not working correctly, which may result, for example, from an unavailable backend database. \n\nCheck if the backend database DB_CosNaming (RG NamingServiceDB) is unlocked and active. \n fshascli -s /NamingServiceDB\nIf the NamingServiceDB is locked, unlock it. \n fshascli -u /NamingServiceDB\nAfter a few seconds the database should have restarted and the NaS should have automatically re-established connections. Ensure the restart and the re-established connections by issuing the ns_listall commands mentioned above.\n\nIf this does not solve the problem, there is something wrong with the database deployment or configuration. In that case, also the alarm 70156 DISK DATABASE WATCHDOG START-UP FAILED , should be raised by the MySQL DB watchdog dedicated for the DB_CosNaming database instance.		

Table 41-15 BACKPLANE_LINK_FAULTY

Alarm	Attributes	Applicable major release
Name: BACKPLANE_LINK_FAULTY (11612) Type: communicationsAlarm Package: racloms.BACKPLANE_LINK_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BACKPLANE LINK FAULTY Implicitly cleared: true Default probable cause: LAN_ERROR	Release: • LOMS16A
Description: BACKPLANE LINK FAULTY\n\nThe local area network (LAN) monitoring software has declared a backplane\nlink faulty.\n\nThis is a serious condition as the redundancy level of the system is lowered due to the failed link.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check the severity of the alarm. \n\nIf the severity level is WARNING, the system is trying to recover the failed link. No actions are needed at this point.\n\nIf the severity level is MAJOR, there is a backplane link fault. This consists of one of three components, from which it is impossible for the system to distinguish the real cause. The components are:\n\n1. The physical port on the node.\n2. The physical port on the switch.\n3. The physical media between those two ports (i.e. the chassis).\n\nIf the are_resets_enabled parameter is true in the alarm info, the system has already tried to reset the components and the method of repairing the fault is to replace one or more of these components starting from the top.\n\nIf the are_resets_enabled parameter is off, it means that no automatic resets have been executed on these components and manual resets could be beneficial as instructed in the hardware maintenance documentation. The name and location of the node is included in the application additional info. \n\nRefer to the hardware maintenance documentation for how to change faulty components.\n\nAfter replacing any of the components and powering on the system or restarting a component, allow the system at least five (5) minutes to stabilize the fault information. During this time, other alarms might appear and the alarm might be cancelled for a while but it does not react to other alarms.		

Table 41-16 BACKUP_AND_RESTORE_CONNECTION_TO_NETACT_LOST

Alarm	Attributes	Applicable major release
Name: BACKUP_AND_RESTORE_CONNECTION_TO_NETACT_LOST (11613) Type: communicationsAlarm Package: racloms.BACKUP_AND_RESTORE_CONNECTION_TO_NETACT_LOST Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BACKUP AND RESTORE CONNECTION TO NETACT LOST Implicitly cleared: true Default probable cause: UNAVAILABLE	Release: • LOMS16A
Description: BACKUP AND RESTORE CONNECTION TO NETACT LOST\n\nRemote backup and restore operation was not able to send a reply to NetAct because of lost connection/communication to NetAct. This alarm informs the operator about a problem on OMS - NetAct communication which means that OMS message reply is not sent to NetAct.\n\nNetAct is not able to receive message from Nwi3BackupRestore. NetAct waits until it reaches timeout.\n\nThe system clears the alarm automatically when the fault has been corrected as presented in INSTRUCTIONS.		
Remedial action: Check communication between OMS and NetAct then restart Nwi3BackupRestore process on OMS [alarm is cleared automatically].		

Table 41-17 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • LOMS16A
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 41-18 BLADECENTER_BLOWER_SPEED_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: BLADECENTER_BLOWER_SPEED_OUT_ OF_LIMIT (11614) Type: equipmentAlarm Package: racloms.BLADECENTER_BLOWER_ SPEED_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER BLOWER SPEED OUT OF LIMIT Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BLADECENTER BLOWER SPEED OUT OF LIMIT\n\nThe reading of a single Intelligent Platform Management Interface (IPMI) fan sensor is out of limit. The rotation speed of a fan group is either low or abnormally high.\n\nHigh speed may indicate a temperature-related problem which might eventually cause hardware management to automatically shut down the plug-in units to prevent any physical damage to them.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the IBM BladeCenter Hardware Maintenance Manual and Troubleshooting Guide (ID MIGR-50053) for instructions at manufacturer's WWW pages http://www.ibm.com. \n2. If the problem remains, contact your local Nokia representative.		

Table 41-19 BLADECENTER_INCOMPATIBLE_HARDWARE_CONFIGURATION

Alarm	Attributes	Applicable major release
Name: BLADECENTER_INCOMPATIBLE_ HARDWARE_CONFIGURATION (11615) Type: equipmentAlarm Package: racloms.BLADECENTER_INCOMPATIBLE_ HARDWARE_CONFIGURATION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER INCOMPATIBLE HARDWARE CONFIGURATION Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BLADECENTER INCOMPATIBLE HARDWARE CONFIGURATION\n\nIncompatible hardware configuration has been detected.\n\nConfiguration of a hardware contains a severe incompatibility problem. This may cause, for example, a blade to be inaccessible.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-19 BLADECENTER_INCOMPATIBLE_HARDWARE_CONFIGURATION (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Check the IBM BladeCenter Hardware Maintenance Manual and Troubleshooting Guide (ID MIGR-50053) for instructions at manufacturer's WWW pages http://www.ibm.com. \n2. If the problem remains, contact your local Nokia representative.\ nYou can find the details of the faulty plug-in unit in the Identifying Application Additional Info field of the alarm.		

Table 41-20 BLADECENTER_MANAGEMENT_MODULE_REDUNDANCY_LOST

Alarm	Attributes	Applicable major release
Name: BLADECENTER_MANAGEMENT_MODULE_ REDUNDANCY_LOST (11616) Type: equipmentAlarm Package: racloms.BLADECENTER_MANAGEMENT_ MODULE_REDUNDANCY_LOST Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER MANAGEMENT MODULE REDUNDANCY LOST Implicitly cleared: true Default probable cause: LOST_REDUNDANCY	Release: • LOMS16A
Description: BLADECENTER MANAGEMENT MODULE REDUNDANCY LOST\n\nOne of the management modules has failed or has been removed from the system. The active management module is still operational.\n\nThe system is fully operational with only a single management module. However, the faulty or removed management module should be replaced as soon as possible to ensure fault tolerant operability. If the redundant management module is not replaced and the active one fails, the whole system becomes inoperable.\n\nThe alarm is automatically cleared by the operating system's fault detector when a working management module is re-inserted in the chassis.		
Remedial action: 1. If there is only one management module present in the chassis, insert another module in the chassis to ensure fault tolerant operability. Check the IBM BladeCenter Advanced Management Module Installation Guide (ID MIGR-63781) for instructions in the manufacturer's WWW pages at http://www.ibm.com.\n\n2. If both management modules are present, try removing and re-inserting the standby management module. Check the IBM BladeCenter Troubleshooting Management Module issues (ID MIGR-58898) for instructions in the manufacturer's WWW pages at http://www.ibm.com. If the problem persists, replace the standby management module with a new one.\nIf the previous steps have not resolved the situation, contact your local Nokia representative.		

Table 41-21 BLADECENTER_PLUG_IN_UNIT_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER_PLUG_IN_UNIT_FAILURE (11617) Type: equipmentAlarm Package: racloms.BLADECENTER_PLUG_IN_UNIT_ FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER PLUG-IN UNIT FAILURE Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BLADECENTER PLUG-IN UNIT FAILURE\n\nA fatal failure in the plug-in unit hardware has been detected.\n\nThere is a severe fault in the plug-in unit hardware. This may cause, for example, hardware management to automatically shut down the plug-in unit to prevent any physical damage to it.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the IBM BladeCenter Hardware Maintenance Manual and Troubleshooting Guide (ID MIGR-50053) for instructions at manufacturer's WWW pages http://www.ibm.com.\n2. If the problem remains, contact your local Nokia representative to replace the plug-in unit. Note that replacing an operational disk drive may cause loss of data.\nYou can find the details of the faulty plug-in unit in the Identifying Application Additional Info field of the alarm.		

Table 41-22 BLADECENTER_PLUG_IN_UNIT_TEMPERATURE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: BLADECENTER_PLUG_IN_UNIT_ TEMPERATURE_OUT_OF_LIMIT (11618) Type: equipmentAlarm Package: racloms.BLADECENTER_PLUG_IN_UNIT_ TEMPERATURE_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER PLUG-IN UNIT TEMPERATURE OUT OF LIMIT Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BLADECENTER PLUG-IN UNIT TEMPERATURE OUT OF LIMIT\n\nThe reading of a single Intelligent Platform Management Interface (IPMI) temperature sensor is out of limit.\n\nIf the alarm is constantly raised, there is a severe temperature-related problem and the plug-in unit may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the IBM BladeCenter Hardware Maintenance Manual and Troubleshooting Guide (ID MIGR-50053) for instructions at manufacturer's WWW pages http://www.ibm.com.\n2. If the problem remains, contact your local Nokia representative.\ nYou can find the details of the faulty plug-in unit in the Identifying Application Additional Info field of the alarm.		

Table 41-23 BLADECENTER_PLUG_IN_UNIT_VOLTAGE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: BLADECENTER_PLUG_IN_UNIT_VOLTAGE_ OUT_OF_LIMIT (11619) Type: equipmentAlarm Package: racloms.BLADECENTER_PLUG_IN_UNIT_ VOLTAGE_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER PLUG-IN UNIT VOLTAGE OUT OF LIMIT Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADECENTER PLUG-IN UNIT VOLTAGE OUT OF LIMIT\n\nThe reading of a single Intelligent Platform Management Interface (IPMI) voltage sensor is out of limit.\n\nIf the alarm is constantly raised, there is a severe hardware problem and the plug-in unit may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the IBM BladeCenter Hardware Maintenance Manual and Troubleshooting Guide (ID MIGR-50053) for instructions at manufacturer's WWW pages http://www.ibm.com.\n2. If the problem remains, contact your local Nokia representative.\ nYou can find the details of the faulty plug-in unit in the Identifying Application Additional Info field of the alarm.		

Table 41-24 BLADECENTER_POWER_SUPPLY_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER_POWER_SUPPLY_FAILURE (11620) Type: equipmentAlarm Package: racloms.BLADECENTER_POWER_ SUPPLY_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER POWER SUPPLY FAILURE Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A

Table 41-24 BLADECENTER_POWER_SUPPLY_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: BLADECENTER POWER SUPPLY FAILURE\n\nThere is a failure in one of the power modules.\n\nIf all the power entry modules are down, it results in degraded chassis power supply redundancy, or total loss of power.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application additional info" (spTrapEvtName) of the alarm, find the exact cause from IBM reference documentation available at the following site: http://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n\n2. Perform the actions mentioned in the "User Response" section of the IBM reference documents.		

Table 41-25 BLADECENTER__BLADE_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER__BLADE_FAILURE (11621) Type: equipmentAlarm Package: racloms.BLADECENTER__BLADE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER: BLADE FAILURE Implicitly cleared: true Default probable cause: EXTERNAL_EQUIPMENT_FAILURE	Release: • LOMS16A
Description: BLADECENTER: BLADE FAILURE\n\nOne of the Blades has malfunctioned.\n\nThe system's boot process for the specified blade server, failed before the operating system was loaded.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application additional info" (spTrapEvtName) of the alarm, find the exact cause from IBM reference documentation available at the following site: \nhttp://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n2. Perform the actions mentioned in the "User Response" section of the IBM reference documents.		

Table 41-26 BLADECENTER__CHASSIS_SYSTEM_MANAGEMENT_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER__CHASSIS_SYSTEM_MANAGEMENT_FAILURE (11622) Type: equipmentAlarm Package: racloms.BLADECENTER__CHASSIS_SYSTEM_MANAGEMENT_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER: CHASSIS/SYSTEM MANAGEMENT FAILURE Implicitly cleared: true Default probable cause: EXTERNAL_EQUIPMENT_FAILURE	Release: • LOMS16A

Table 41-26 BLADECENTER__CHASSIS_SYSTEM_MANAGEMENT_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: BLADECENTER: CHASSIS/SYSTEM MANAGEMENT FAILURE\n\nSome hardware component in the Chassis has malfunctioned or has stopped working.\n\nThere can be multiple effects of this alarm. For example:\n\nThe advanced management module may not be able to determine the management module bay in which it is installed. Therefore, it may use management module bay 1 as the installed bay.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application additional info" (spTrapEvtName) of the alarm, find the exact cause from IBM reference documentation available at the following site: \nhttp://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n 2. Perform the actions mentioned in the "User Response" section of the IBM reference documents.		

Table 41-27 BLADECENTER__COOLING_DEVICE_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER__COOLING_DEVICE_FAILURE (11623) Type: environmentalAlarm Package: racloms.BLADECENTER__COOLING_DEVICE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER: COOLING DEVICE FAILURE Implicitly cleared: true Default probable cause: COOLING_SYSTEM_FAILURE	Release: • LOMS16A
Description: BLADECENTER: COOLING DEVICE FAILURE\n\nThe specified fan or blower module is no longer operating.\n\nThe hardware component where the fan module is not operating, may stop functioning due to overheating.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application\nadditional info" (spTrapEvtName) of the alarm, find the exact cause\nfrom IBM reference documentation available at the following site: \n\nhttp://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n 2. Perform the actions mentioned in the "User Response" section\nof the IBM reference documents.		

Table 41-28 BLADECENTER__I_O_MODULE_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER__I_O_MODULE_FAILURE (11624) Type: equipmentAlarm Package: racloms.BLADECENTER__I_O_MODULE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER: I/O MODULE FAILURE Implicitly cleared: true Default probable cause: EXTERNAL_EQUIPMENT_FAILURE	Release: • LOMS16A

Table 41-28 BLADECENTER__I_O_MODULE_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: BLADECENTER: I/O MODULE FAILURE\n\nOne of the I/O (Input/Ouput) module has failed,or is malfunctioning.\n\nThe advanced management module is unable to read the status of the specified I/O module due to a fault.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application additional info" (spTrapEvtName) of the alarm, find the exact cause from IBM reference documentation available at the following site: \nhttp://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n \n2. Perform the actions mentioned in the "User Response" section of the IBM reference documents.		

Table 41-29 BLADECENTER__STORAGE_MODULE_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADECENTER__STORAGE_MODULE_FAILURE (11625) Type: equipmentAlarm Package: racloms.BLADECENTER__STORAGE_MODULE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADECENTER: STORAGE MODULE FAILURE Implicitly cleared: true Default probable cause: EXTERNAL_EQUIPMENT_FAILURE	Release: • LOMS16A
Description: BLADECENTER: STORAGE MODULE FAILURE\n\nOne of the Storage modules has stopped working, or has malfunctioned.\n\nA fault has occurred in the battery backup unit used to back up the cache for the specified SAS (Serial Attached SCSI) RAID controller module.\n\nIn the IBM Reference documentation, Chapter 2 contains information on mapping of the event codes against the exact cause of the alarm. \n\nFor information on clearing the alarm, refer to the 'Recoverable' section of the reference documents. If the Recoverable section says 'yes', it means that the alarm generated will be automatically cleared. If the Recoverable section says 'no', the alarm has to be manually cleared using the alarm management application.		
Remedial action: 1. With the help of the Event code displayed in "Identifying Application\nadditional info" (spTrapEvtName) of the alarm, find the exact cause\nfrom IBM reference documentation available at the following site: \nhttp://publib.boulder.ibm.com/infocenter/bladectr/documentation/topic/com.ibm.bladecenter.advmgtmod.doc/kp1avAMMMessagesGuide.pdf\n\n2. Perform the actions mentioned in the "User Response" section\nof the IBM reference documents.		

Table 41-30 BLADESYSTEM_CHASSIS_POWER_PROBLEM

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_CHASSIS_POWER_PROBLEM (11626) Type: equipmentAlarm Package: racloms.BLADESYSTEM_CHASSIS_POWER_PROBLEM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM CHASSIS POWER PROBLEM Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A

Table 41-30 BLADESYSTEM_CHASSIS_POWER_PROBLEM (continued)

Alarm	Attributes	Applicable major release
Description: BLADESYSTEM CHASSIS POWER PROBLEM\n\nEither the input power limit to the power subsystem AC facility has been exceeded for this enclosure, or there is a DC power problem.\n\nThe system is still usable, but the power enclosure should be checked as soon as possible to ensure fault tolerant operability.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the power enclosure and power supplies. Replace any failed or degraded power supplies.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-31 BLADESYSTEM_FAN_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_FAN_FAILURE (11627) Type: equipmentAlarm Package: racloms.BLADESYSTEM_FAN_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM FAN FAILURE Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BLADESYSTEM FAN FAILURE\n\nThe enclosure fan status has been set to 'failed' or 'degraded' or a fan has been removed. If the status has been set to failed no other operating fans exist in the redundant fan group. If the status has been set to degraded, an enclosure fan has failed, but other fans in the redundant fan group are still operating.\n\nThis may result in overheating of the enclosure.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check all fans and replace the removed or defective fans as soon as possible.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-32 BLADESYSTEM_FUSE_OPEN

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_FUSE_OPEN (11628) Type: equipmentAlarm Package: racloms.BLADESYSTEM_FUSE_OPEN Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM FUSE OPEN Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM FUSE OPEN\n\nFuse open. The fuse has been tripped.\n\nThe server blade loses power and any activity on the server operating system will be lost.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check enclosure and/or blade power connections and reset the fuse. \nCheck the HP BladeSystem p-Class 1U power enclosure technology brief for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-33 BLADESYSTEM_INTERCONNECT_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_INTERCONNECT_FAILURE (11629) Type: equipmentAlarm Package: racloms.BLADESYSTEM_ INTERCONNECT_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM INTERCONNECT FAILURE Implicitly cleared: true Default probable cause: LOST_REDUNDANCY	Release: • LOMS16A
Description: BLADESYSTEM INTERCONNECT FAILURE\n\nThe interconnect status has been set to 'failed' or 'degraded' or the interconnect has been removed.\n\nThe connectability of the system has been compromised.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Replace the interconnect as soon as possible.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-34 BLADESYSTEM_LINE_VOLTAGE_PROBLEM

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_LINE_VOLTAGE_PROBLEM (11630) Type: equipmentAlarm Package: racloms.BLADESYSTEM_LINE_VOLTAGE_ PROBLEM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM LINE VOLTAGE PROBLEM Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM LINE VOLTAGE PROBLEM\n\nThe rack power supply has detected an input line voltage problem.\n\nIf the alarm is set off constantly, there is a severe hardware problem and the server blade may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the power input for the power supply and replace any failed power supplies.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-35 BLADESYSTEM_ONBOARD_ADMINISTRATOR_REDUNDANCY_LOST

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_ONBOARD_ ADMINISTRATOR_REDUNDANCY_LOST (11631) Type: equipmentAlarm Package: racloms.BLADESYSTEM_ONBOARD_ ADMINISTRATOR_REDUNDANCY_LOST Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM ONBOARD ADMINISTRATOR REDUNDANCY LOST Implicitly cleared: true Default probable cause: LOST_REDUNDANCY	Release: • LOMS16A
Description: BLADESYSTEM ONBOARD ADMINISTRATOR REDUNDANCY LOST\n\nThe Onboard Administrator has been removed or its status has been set to 'degraded'.\n\nThis alarm signifies that an Onboard Administrator has been removed or it has failed but the other Onboard Administrator is still operating.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-35 BLADESYSTEM_ONBOARD_ADMINISTRATOR_REDUNDANCY_LOST (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Replace the Onboard Administrator as soon as possible.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-36 BLADESYSTEM_POWER_CHASSIS_NOT_LOAD_BALANCED

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_CHASSIS_NOT_LOAD_BALANCED (11632) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_CHASSIS_NOT_LOAD_BALANCED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER CHASSIS NOT LOAD BALANCED Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER CHASSIS NOT LOAD BALANCED\n\nPower subsystem not load balanced.\n\nThe system is still usable, but the power enclosure should be checked as soon as possible to ensure fault tolerant operability.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the power enclosure and power supplies. Replace any failed or degraded power supplies. Add additional power supplies if needed.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-37 BLADESYSTEM_POWER_ON_FAILED

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_ON_FAILED (11633) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_ON_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER ON FAILED Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER ON FAILED\n\nInadequate power to turn on.\n\nThere is not enough power to power up the server blade, or not enough power to power it up while maintaining redundancy for the other blades in the enclosure.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check power connections or add power supplies.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-38 BLADESYSTEM_POWER_SHED_AUTO_SHUTDOWN

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_SHED_AUTO_SHUTDOWN (11634) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_SHED_AUTO_SHUTDOWN Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER SHED AUTO SHUTDOWN Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER SHED AUTO SHUTDOWN\n\nThe server blade was shutdown due to a lack of power.\n\nThe server blade is out of use.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check power connections or add power supplies.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-39 BLADESYSTEM_POWER_SUBSYSTEM_NOT_REDUNDANT

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_SUBSYSTEM_NOT_REDUNDANT (11635) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_SUBSYSTEM_NOT_REDUNDANT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER SUBSYSTEM NOT REDUNDANT Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER SUBSYSTEM NOT REDUNDANT\n\nRack power supply not redundant.\n\nThe rack power subsystem is no longer in a redundant state.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Replace any failed or degraded power supplies to return the system to a redundant state.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-40 BLADESYSTEM_POWER_SUBSYSTEM_OVERLOAD_CONDITION

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_SUBSYSTEM_OVERLOAD_CONDITION (11636) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_SUBSYSTEM_OVERLOAD_CONDITION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER SUBSYSTEM OVERLOAD CONDITION Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER SUBSYSTEM OVERLOAD CONDITION\n\nThe rack power subsystem has an overload condition.\n\nThe system is still usable, but in order to ensure full fault tolerant operability any failed power supplies should be replaced as soon as possible.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-40 BLADESYSTEM_POWER_SUBSYSTEM_OVERLOAD_CONDITION (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Replace any failed power supplies as soon as possible to return the system to a redundant state. \nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-41 BLADESYSTEM_POWER_SUPPLY_FAILURE

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_POWER_SUPPLY_FAILURE (11637) Type: equipmentAlarm Package: racloms.BLADESYSTEM_POWER_SUPPLY_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM POWER SUPPLY FAILURE Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM POWER SUPPLY FAILURE\n\nA power supply has been removed or the power supply status has been set to 'failed' or 'degraded'.\n\nDepending on the alarm severity, this alarm signifies that a power supply has been removed (WARNING severity), degraded (MAJOR) or failed (CRITICAL).\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Replace the power supply as soon as possible.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-42 BLADESYSTEM_REMOTE_INSIGHT_BATTERY_FAILED

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_REMOTE_INSIGHT_BATTERY_FAILED (11638) Type: equipmentAlarm Package: racloms.BLADESYSTEM_REMOTE_INSIGHT_BATTERY_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM REMOTE INSIGHT BATTERY FAILED Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: BLADESYSTEM REMOTE INSIGHT BATTERY FAILED\n\nThe Remote Insight battery has failed.\n\niLO 2 remote control and management functionality may become unavailable.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Replace the Remote Insight battery. Check the HP ProLiant BL465c Server Blade Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com. \n\n2. If the problem persists, contact your local NSN representative.		

Table 41-43 BLADESYSTEM_REMOTE_INSIGHT_ERROR

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_REMOTE_INSIGHT_ERROR (11639) Type: equipmentAlarm Package: racloms.BLADESYSTEM_REMOTE_INSIGHT_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM REMOTE INSIGHT ERROR Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: BLADESYSTEM REMOTE INSIGHT ERROR\n\nThe host operating system has detected an error in the Remote Insight/ Integrated Lights-Out interface or the Remote Insight/ Integrated Lights-Out firmware has detected a Remote Insight self test error.\n\nThe Remote Insight/ Integrated Lights-Out control and management functionality may not be completely available.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Contact your local NSN representative.		

Table 41-44 BLADESYSTEM_REMOTE_INSIGHT_POWER_OUTAGE

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_REMOTE_INSIGHT_POWER_OUTAGE (11640) Type: equipmentAlarm Package: racloms.BLADESYSTEM_REMOTE_INSIGHT_POWER_OUTAGE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM REMOTE INSIGHT POWER OUTAGE Implicitly cleared: false Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: BLADESYSTEM REMOTE INSIGHT POWER OUTAGE\n\nThe Remote Insight/ Integrated Lights-Out firmware has detected server power failure.\n\nThe server blade is out of power.\n\nClear the alarm with an alarm management application after correcting the fault as presented in INSTRUCTIONS.		
Remedial action: 1. Check that the blade has not been powered off and verify the power inputs and supplies.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-45 BLADESYSTEM_TEMPERATURE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_TEMPERATURE_OUT_OF_LIMIT (11641) Type: equipmentAlarm Package: racloms.BLADESYSTEM_TEMPERATURE_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM TEMPERATURE OUT OF LIMIT Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: BLADESYSTEM TEMPERATURE OUT OF LIMIT\n\nThe enclosure temperature status has been set to 'failed' or 'degraded'. If the status has been set to degraded, an enclosure temperature sensor has been tripped indicating a possible overheat condition. If the status has been set to failed, an enclosure temperature sensor has been tripped indicating an overheat condition.\n\nIf the alarm is set off constantly, there is a severe temperature-related problem and the server blade may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-45 BLADESYSTEM_TEMPERATURE_OUT_OF_LIMIT (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Shutdown the enclosure and possibly the rack as soon as possible. Ensure all fans are working properly and that air flow in the rack has not been blocked.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-46 BLADESYSTEM_UNKNOWN_POWER_CONSUMPTION

Alarm	Attributes	Applicable major release
Name: BLADESYSTEM_UNKNOWN_POWER_CONSUMPTION (11642) Type: equipmentAlarm Package: racloms.BLADESYSTEM_UNKNOWN_POWER_CONSUMPTION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLADESYSTEM UNKNOWN POWER CONSUMPTION Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: BLADESYSTEM UNKNOWN POWER CONSUMPTION\n\nThere is an unknown power consumer drawing power.\n\nUnknown power consumption may result in degraded chassis power supply redundancy or total loss of power.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check the power enclosure and power supplies. Replace any failed or degraded power supplies.\nCheck the HP BladeSystem Enclosure Maintenance and Service Guide for instructions in the manufacturer's WWW pages at http://www.hp.com.\n\n2. If the problem persists, contact your local NSN representative.		

Table 41-47 BLOCK_STORAGE_FOR_ADDITIONAL_PARTITION_MISSING

Alarm	Attributes	Applicable major release
Name: BLOCK_STORAGE_FOR_ADDITIONAL_PARTITION_MISSING (11643) Type: processingErrorAlarm Package: racloms.BLOCK_STORAGE_FOR_ADDITIONAL_PARTITION_MISSING Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BLOCK STORAGE FOR ADDITIONAL PARTITION MISSING Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: BLOCK STORAGE FOR ADDITIONAL PARTITION MISSING\n\nSome of partitions are missing additional bock storage\n\nAdditional OMS partition is not accessible because of missing storage block device.\n\nOMS system clears the alarm automatically whenever partition storage is recovered.		
Remedial action: Check the additional information for maintenance action details		

Table 41-48 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LOMS16A

Table 41-48 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 41-49 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 41-50 BOOTING_FAILURE

Alarm	Attributes	Applicable major release
Name: BOOTING_FAILURE (11644) Type: equipmentAlarm Package: racloms.BOOTING_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BOOTING FAILURE Implicitly cleared: false Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: BOOTING FAILURE\n\nA booting failure has taken place. \n\nPossible causes are:\nNo bootable media\nThe pre-boot execution environment (PXE) server is not found\nInvalid boot sector\nTimeout waiting for user selection of boot source\n\nThe unit boot-up may be failing.\n\nClear the alarm with the alarm management application after correcting the fault, according to the instructions.		
Remedial action: 1. Try to restart the unit.\n\n2. Select the boot source at the prompt.\n\n3. Check that boot media exists.\n\n4. Check the validity of the boot media (such as, the disk is bootable or the PXE server is available).\n\n5. If the problem remains after following these instructions, please contact your local customer support.		

Table 41-51 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • LOMS16A
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 41-52 BTS_O_M_TOTAL_CONNECTION_LIMIT_EXCEEDED

Alarm	Attributes	Applicable major release
Name: BTS_O_M_TOTAL_CONNECTION_LIMIT_EXCEEDED (11645) Type: processingErrorAlarm Package: racloms.BTS_O_M_TOTAL_CONNECTION_LIMIT_EXCEEDED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: BTS O&M TOTAL CONNECTION LIMIT EXCEEDED Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: BTS O&M TOTAL CONNECTION LIMIT EXCEEDED\n\nNumber of connected network elements has exceeded the maximum allowed value.\n\nFurther connection attempts to the OMS are rejected.\n\nDo not clear the alarm. The system cancels the alarm automatically after its lifetime has elapsed or the problem has been solved.		
Remedial action: Disconnect the network elements which exceeded the maximum allowed connection limit.		

Table 41-53 CANNOT_WRITE_TO_DISK

Alarm	Attributes	Applicable major release
Name: CANNOT_WRITE_TO_DISK (11646) Type: equipmentAlarm Package: racloms.CANNOT_WRITE_TO_DISK Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CANNOT WRITE TO DISK Implicitly cleared: true Default probable cause: DISK_PROBLEM	Release: • LOMS16A

Table 41-53 CANNOT_WRITE_TO_DISK (continued)

Alarm	Attributes	Applicable major release
Description: CANNOT WRITE TO DISK\n\nDisk write operation fails because the disk is inoperable or partially full.\n\nLog entries or data structure image cannot be written to disk. Data structure can be read but update operations are not accepted until the disk is writable.\n\nThe system automatically clears the alarm when the fault has been corrected.		
Remedial action: This problem is directly related to disk problems. Use the df command to check if the disk partition is full. The mount point can be seen in the File name field of this alarm. After the next checkpoint of the FDS, there should be more space on the disk, because the FDS log files are purged. The checkpoint is taken on the basis of time, successful update, or number of updates, depending on the configuration.\n\nIf the problem cannot be solved otherwise, contact your local Nokia representative and provide them with the information you obtained from alarm notification's fields.		

Table 41-54 CAPACITY_USAGE_WARNING_LIMIT_IS_REACHED

Alarm	Attributes	Applicable major release
Name: CAPACITY_USAGE_WARNING_LIMIT_IS_REACHED (11647) Type: qualityOfServiceAlarm Package: racloms.CAPACITY_USAGE_WARNING_LIMIT_IS_REACHED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CAPACITY USAGE WARNING LIMIT IS REACHED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: CAPACITY USAGE WARNING LIMIT IS REACHED\n\nThis is an informative alarm which indicates that a capacity usage level of a licensed feature has reached one of its predefined warning limits: the capacity usage warning limit or the full capacity limit. \n\nFor each warning limit there is a corresponding alarm severity. The alarm severity increases as the warning limit becomes closer to the full capacity limit.\n\nIf a warning limit with value less than 100% is reached, this alarm has no effect. If the full capacity limit (100%) is reached, the application implementing the licensed feature may stop operating.\n\nThe alarm is cleared automatically if a new licence with additional capacity has been installed or the capacity usage has been decreased. \n\nOtherwise, manual clearing is required; clear the alarm with alarm management application after correcting the fault as presented in Instructions.		
Remedial action: Verify the licensed capacity for the feature. If the feature requires additional capacity, install a new licence. \n\n\n1. To check the amount of currently used licensed capacity execute following command:\n lmcli getFeatureCapacityUsage <FeatureCode> \n\nwhere <FeatureCode> is the code of the feature to be checked. \n\n2. If it is necessary to increase the capacity, a new licence has to be installed. To install a licence execute following command:\n\n lmcli importLicence <LicenceFilename> \n\nwhere <LicenceFilename> is a fully qualified filename of the licence file to be installed.\n\n3. In case of a false alarm, fill in the problem report and send it to your local Nokia representative.		

Table 41-55 CERTIFICATES_DISCREPANCY

Alarm	Attributes	Applicable major release
Name: CERTIFICATES_DISCREPANCY (11648) Type: processingErrorAlarm Package: racloms.CERTIFICATES_DISCREPANCY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CERTIFICATES DISCREPANCY Implicitly cleared: true Default probable cause: VERSION_MISMATCH	Release: • LOMS16A

Table 41-55 CERTIFICATES_DISCREPANCY (continued)

Alarm	Attributes	Applicable major release
Description: CERTIFICATES DISCREPANCY\n\nThis alarm indicates that CA certificate received in TLS connection differs from CA certificate with the same issuer name and subject name which is installed in OMS (e.g. it has been installed in OMS to support CRL Distribution Point parameter defined in OMS for downloading related CRL).\nMost likely other NE uses newer CA certificate and it should be installed manually in OMS as well.\n\nThere is a risk that CRL being in usage, formerly downloaded to OMS, is not up to date or its validation in the next CRL download might fail with the old CA certificate present in OMS.\n\nClear the alarm with the alarm management application after checking correctness of the CA certificate and CRL Distribution Point parameter		
Remedial action: Perform the following actions:\n\n1. Verify certificate in question which is installed in OMS and on the other NE, then install a new version of CA certificate in OMS if needed.\n2. If CA certificate installation was required in OMS then verify related CRL Distribution Point parameter (if it had been defined in OMS) and update it if needed.\n3. If CRL Distribution point parameter has been changed then initiate CRL update operation.		

Table 41-56 CERTIFICATE_CAPACITY_REACHED

Alarm	Attributes	Applicable major release
Name: CERTIFICATE_CAPACITY_REACHED (11649) Type: qualityOfServiceAlarm Package: racloms.CERTIFICATE_CAPACITY_REACHED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CERTIFICATE CAPACITY REACHED Implicitly cleared: true Default probable cause: RESOURCE_AT_OR_NEARING_CAPACITY	Release: • LOMS16A
Description: CERTIFICATE CAPACITY REACHED\n\nThis alarm is raised when its own CA certificate storage capacity or CRL storage space is about to be reached.\n\nCA Certificate or CRL storage capacity was reached, so new certificate or CRL cannot be installed.\n\nThe alarm is cleared automatically by the alarm system after CA certificate storage capacity is below its minimum acceptable limit (i.e. unnecessary or invalid certificates are deleted) or CRLs are within the acceptable disk space limit.		
Remedial action: OMS detected excess of certificates in its own CA certificate storage capacity or excess of CRLs in disk storage space. In order to clear this alarm any new certificate exceeding the quantity of 12 certificates shall be deleted.		

Table 41-57 CERTIFICATE_EXPIRED

Alarm	Attributes	Applicable major release
Name: CERTIFICATE_EXPIRED (11650) Type: processingErrorAlarm Package: racloms.CERTIFICATE_EXPIRED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CERTIFICATE EXPIRED Implicitly cleared: true Default probable cause: TIMEOUT_EXPIRED	Release: • LOMS16A
Description: CERTIFICATE EXPIRED\n\nThis alarm is raised when its own EE or intermediate CA or root CA certificate expires.\n\nThe alarm may have effect on the OMS security. Expired certificates cannot be used, so secure connections will not work.\n\nAlarm will be cleared automatically after a new certificate with proper lifetime is installed to the system.		
Remedial action: The operator should install a new certificate with proper lifetime as soon as possible.		

Table 41-58 CERTIFICATE_EXPIRING

Alarm	Attributes	Applicable major release
Name: CERTIFICATE_EXPIRING (11651) Type: processingErrorAlarm Package: racloms.CERTIFICATE_EXPIRING Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CERTIFICATE EXPIRING Implicitly cleared: true Default probable cause: TIMEOUT_EXPIRED	Release: • LOMS16A
Description: CERTIFICATE EXPIRING\n\nThe alarm means that End Entity (EE) or Certificate Authority (CA) certificate expiry is close.\n\nIt will not be possible to use expired certificate. Secure connection will not be working. At the worst case the whole OMS will not be functioning.\n\nAlarm will be cleared automatically by the alarm system after a new certificate with proper lifetime is installed to the system.		
Remedial action: The operator should install a new certificate with proper lifetime as soon as possible.		

Table 41-59 CERTIFICATE_REVOKED

Alarm	Attributes	Applicable major release
Name: CERTIFICATE_REVOKED (11652) Type: processingErrorAlarm Package: racloms.CERTIFICATE_REVOKED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CERTIFICATE REVOKED Implicitly cleared: true Default probable cause: TIMEOUT_EXPIRED	Release: • LOMS16A
Description: CERTIFICATE REVOKED\n\nThe alarm is raised if the Network Element certificate cannot be validated against Certificate Revocation List (CRL). It means certificate is not valid anymore.\n\nThe alarm may have effect on the OMS security. The revoked certificate cannot be used.\n\nThe alarm is cleared in case of successful certificate validation against CRL.		
Remedial action: The operator should provide new valid NE certificate.		

Table 41-60 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • LOMS16A
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 41-61 CLUSTER_OPERATION_INITIATED_BY_OPERATOR

Alarm	Attributes	Applicable major release
Name: CLUSTER_OPERATION_INITIATED_BY_ OPERATOR (11653) Type: qualityOfServiceAlarm Package: racloms.CLUSTER_OPERATION_ INITIATED_BY_OPERATOR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CLUSTER OPERATION INITIATED BY OPERATOR Implicitly cleared: true Default probable cause: CONGESTION	Release: • LOMS16A
Description: CLUSTER OPERATION INITIATED BY OPERATOR\n\nThis is an informative alarm which indicates that an operator has initiated\na cluster operation on the specified managed object (MO). The MO can be to the whole cluster, a node, a recovery unit (RU), or a process. The platform high availability services (HAS) is now executing the operation. The operation can be\n- switchover\n- restart\n- power-off.\n\nThe operations have different effects: \n\nSwitchover \n- Applicable only to recovery groups (RG). The active RU instance of the RG is terminated and a standby instance on another node started or, in case of a hot active standby RG, activated. The service provided by the named RU is down until the switchover is complete. \n\nRestart \n- For the cluster and nodes this means a physical restart (reboot) of node(s). For other MOs, the named MO is stopped and restarted. The services provided by the named MO are down during the restart.\n\nPower-off \n- Applicable only to nodes. The named node is being powered off.\n\nThe alarm system clears the alarm automatically after its time to live has expired.		
Remedial action: This is an informative alarm and does not require any actions.		

Table 41-62 CLUSTER_STARTED__RESTARTED_

Alarm	Attributes	Applicable major release
Name: CLUSTER_STARTED__RESTARTED_ (11654) Type: processingErrorAlarm Package: racloms.CLUSTER_STARTED__ RESTARTED_ Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CLUSTER STARTED (RESTARTED) Implicitly cleared: false Default probable cause: SOFTWARE_ ENVIRONMENT_PROBLEM	Release: • LOMS16A
Description: CLUSTER STARTED (RESTARTED)\n\nThe whole cluster is starting or restarting.\n\nStarting or restarting of the whole cluster means (re)starting of all managed objects within the cluster.\nThe (re)start may have been initiated by an operator or be caused by fatal errors in some critical hardware or software component.\nWhen the cluster is restarted, the alarm system clears all alarms that were raised by the cluster's managed objects before the restart.\n\nClear the alarm after carefully checking the alarm status in the cluster.		
Remedial action: This alarm is an informative alarm indicating that the whole cluster has been (re)started. As this operation is critical for software and hardware, check carefully the alarm status in the cluster after the restart.		

Table 41-63 CMP_CERT_RETRIEVAL_FAILURE

Alarm	Attributes	Applicable major release
Name: CMP_CERT_RETRIEVAL_FAILURE (11655) Type: communicationsAlarm Package: racloms.CMP_CERT_RETRIEVAL_ FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CMP CERT RETRIEVAL FAILURE Implicitly cleared: true Default probable cause: TRANSMISSION_ERROR	Release: • LOMS16A

Table 41-63 CMP_CERT_RETRIEVAL_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: CMP CERT RETRIEVAL FAILURE\n\nThe alarm means that the End Entity (EE) certificate was not received from Certificate Authority server, and old EE certificate is used.\n\nNot-trusted certificate might be used.\n\nThe alarm is cleared if OMS has retrieved certificates successfully.		
Remedial action: User should check CMP server parameters in OMS LDAP. If parameters stored in LDAP are correct, the connectivity to CMP server should be also checked. If the above mentioned steps have been done the CMP initialize operation can be repeated.		

Table 41-64 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • LOMS16A
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 41-65 COMPACTING_IN_MEMORY_DATABASE_FAILED

Alarm	Attributes	Applicable major release
Name: COMPACTING_IN_MEMORY_DATABASE_FAILED (11656) Type: processingErrorAlarm Package: racloms.COMPACTING_IN_MEMORY_DATABASE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: COMPACTING IN-MEMORY DATABASE FAILED Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: COMPACTING IN-MEMORY DATABASE FAILED\n\nDefragmentation of the in-memory database is not completed.\n\nThe database is not compacted to reduce memory fragmentation. This does not affect the functioning of the system. In an extreme case, it is possible that some executions may become slower.\n\nThe alarm system clears the alarm automatically after next successful database compact operation.		

Table 41-65 COMPACTING_IN_MEMORY_DATABASE_FAILED (continued)

Alarm	Attributes	Applicable major release
Remedial action: Note: In these instructions TimesTen is referring to the concept in-memory database.\n\n1. Use the parameter management application to check the value of fsdbCompactInterval or fsdbCompactTime for the database in question.\n\n2. After the next compaction operation (as defined in fsdbCompactInterval or fsdbCompactTime), check with the alarm management application if the alarm is still active. \n3. If the compacting failed, check the alarm reason in the application additional information field 2 and continue according to the respective procedures:\n\nIf the reason is TIMEOUT or FAIL:\n\n1. Copy the original master-syslog to the temporary directory:\ncp /var/log/master-syslog /tmp/<filenameA>.<extension>\n(Choose filenameA and extension, for example, 70169_syslog.log)\n\n2. Go to the tmp directory:\ncd /tmp\n\n3. In the node where the alarm was raised, determine the TimesTen status:\nttStatus -v > /tmp/<filenameB>.txt\n(Choose filename, for example, 70169_ttstatus.log; filenameB must be different from the filenameA.)\n\n4. Compress the files with the tar command:\ntar -cf <tarname>.tar <filenameA>.<extension> <filenameB>.txt\n(Choose tarname, for example, 70169.tar.)\n\nNote that the tar command does not delete the original files. When the files are not needed anymore, they can be deleted. \n\n5. Contact your local Nokia representative with the information gathered (<tarname>.tar).\n\n\nIf the reason is ATTRIBUTE:\n\n1. Use the parameter management application to check the values of fsdbCompactInterval and fsdbCompactTime.\n\n2. If the values are correct, follow the procedure for TIMEOUT or FAIL and contact your local Nokia representative with the information described in the TIMEOUT or FAIL section.\n\nIf the values are not correct, proceed as follows:\n\n1. Use the parameter management application to change the values of fsdbCompactInterval, fsdbCompactQuantum, or fsdbCompactTimevalues for the database in question. The database can be found from the entry fsdbFragmentId DB. \n\n2. Perform graceful shutdown to the managed object (MO) of TimesTen Watchdog and start it up to activate the changed parameters.\n\n3. Search the TimesTen Watchdog MO.\nfshascli -v | grep InMemoryDB\n\n4. From the result, search the information of process.\n\n/<node>/FSInMemoryDB<x>Server/TimestenWD<x>\ncommand="(opt/Nokia/SS_DBHAforTT/bin/TimesTenWD <Database Name>)\n\nwhere <node> is the node for which the alarm is raised, <x> is a letter for the distinctive part of the process type name (see Application Id of the alarm), and <Database Name> is the database in question. For example:\n\nProcess /TA-A/FSInMemoryDBaServer/TimesTenWDa\ncommand=(opt/Nokia/SS_DBHAforTT/bin/TimesTenWD DB_Name)\n\n5. Shut down the TimesTen Watchdog process gracefully:\nfshascli -X /<node>/FSInMemoryDB<x>Server/TimesTenWD<x>\n\n6. Start up the TimesTen Watchdog process to activate the parameter values:\nfshascli -u /<node>/FSInMemoryDB<x>Server/TimesTenWD<x>\n\n7. After the next compaction operation, check with alarm management application if the alarm is still active."		

Table 41-66 CONFIGURATION_OF_NWI3_ADAPTER_IS_OUT_OF_ORDER

Alarm	Attributes	Applicable major release
Name: CONFIGURATION_OF_NWI3_ADAPTER_IS_OUT_OF_ORDER (11657) Type: processingErrorAlarm Package: racloms.CONFIGURATION_OF_NWI3_ADAPTER_IS_OUT_OF_ORDER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CONFIGURATION OF NWI3 ADAPTER IS OUT OF ORDER Implicitly cleared: false Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: CONFIGURATION OF NWI3 ADAPTER IS OUT OF ORDER\n\nThe configuration of NWI3 adapter contains invalid attribute values. Depending on the release, the configuration is stored only in the configuration files, or files and LDAP.\n\nThe system ignores the invalid parameters and uses the default values or the closest acceptable value. For example, value 2000 is greater than the highest acceptable value (1440) for heartbeatPeriod (see the table in the Instructions for operator field) and causes this alarm. In this case, 1440 would be used as the heartbeatPeriod.\n\nClear the alarm with an alarm management application after correcting the fault as presented in Instructions.		

Table 41-66 CONFIGURATION_OF_NWI3_ADAPTER_IS_OUT_OF_ORDER (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Correct the invalid attribute value. The attribute name is displayed in the Identifying Application Additional Info field. The name of the configuration file or LDAP branch is displayed in the Application Additional info field. \nThe attributes that can cause this alarm are mainly stored in file /var/opt/Nokia/SS_Nwi3Adapter/config/nwi3mdcorba.ini or LDAP branch fsFragmentId="mediator, fsFragmentId=NWI3, fsClusterId=ClusterRoot. The valid values, as well as the default values, of these attributes are presented in the table below. The attribute names in the LDAP are prefixed with "fsnwi3".\n\nName Type Default\n(fsnwi3)takeIntoUseNext boolean: (0=false,1=true) in nwi3mdcorba.ini and (false,true) in LDAP 0 \n(fsnwi3)registrationServiceIOR string, a valid IOR to NetAct'sregistration service \n(fsnwi3)heartbeatPeriod short, [0..1440], granularity:1 minute 15\n(fsnwi3)reRegistrationPeriod short: [15..1440], \ngranularity:1 minute 60\n(fsnwi3)registrationRetryBasePeriod short: [5..240], \ngranularity:1 minute 15\ n(fsnwi3)retryRandom short: [5..240], \ngranularity:1 minute 5\n(fsnwi3)rePublicationPeriod short [1..60], \ngranularity:1 minute 3\n(fsnwi3)getPublicationServiceRetryPeriod short [1..60], \ngranularity:1 minute 15\n\n2. This alarm can also be caused by the parameter mediatorSessionManagerIOR located in file /var/opt/Nokia/www/SessionManager_V1.ior\nRestart NWI3 adapter to generate mediatorSessionManagerIOR into SessionManager_V1.ior \nIn normal conditions, the restart generates the parameter with the valid value.\n\n3. If the problem is the results from the parameter systemID in file /var/opt/Nokia/www/systemid.txt, the probable cause is that the file systemid.txt is missing. The value in systemID should be the same as in the file. \nCopy /etc/cluster-id to /var/opt/Nokia/www/ systemid.txt and restart the NWI3 adapter."		

Table 41-67 CONFIGURATION_OF_SNMP_MEDIATOR_IS_OUT_OF_ORDER

Alarm	Attributes	Applicable major release
Name: CONFIGURATION_OF_SNMP_MEDIATOR_ IS_OUT_OF_ORDER (11658) Type: processingErrorAlarm Package: racloms.CONFIGURATION_OF_SNMP_ MEDIATOR_IS_OUT_OF_ORDER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CONFIGURATION OF SNMP MEDIATOR IS OUT OF ORDER Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: CONFIGURATION OF SNMP MEDIATOR IS OUT OF ORDER\n\nConfiguration of the SNMP mediator contains values that are unacceptable.\n\nThe invalid part of configuration is ignored. This causes partial loss of functionality. The SNMP traps may be lost.\n\nThe alarm will be cleared automatically by the alarm system after five minutes. If the configuration is still out of order after that, the alarm is raised again.		
Remedial action: Use the parameter management application to correct the configuration branch that is out of order. The Application Additional Information field displays the attribute or entry name that has an unacceptable value. For example, the following entry causes alarm 70001, if xxx is not a hostname that can be resolved:\nfssnmpNEId="xxx,\nfssnmpAttributeType=NEattrs,\ nfssnmpMediatorName=1,fsFragmentId=SNMP,\nfsClusterId=ClusterRoot\nTesting instructions section below provides instructions for creating an invalid entry."		

Table 41-68 CONNECTION_LOST_TO_MASTER_FDS_SERVER

Alarm	Attributes	Applicable major release
Name: CONNECTION_LOST_TO_MASTER_FDS_ SERVER (11659) Type: communicationsAlarm Package: racloms.CONNECTION_LOST_TO_ MASTER_FDS_SERVER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CONNECTION LOST TO MASTER FDS SERVER Implicitly cleared: true Default probable cause: UNAVAILABLE	Release: • LOMS16A

Table 41-68 CONNECTION_LOST_TO_MASTER_FDS_SERVER (continued)

Alarm	Attributes	Applicable major release
Description: CONNECTION LOST TO MASTER FDS SERVER\n\nReplica Fast Data Structure (FDS) server has lost contact to Master FDS server.\n\nUpdates made to Master FDS will not be replicated to this replica until it has been able to reconnect to Master FDS Server.\n\nWhen Replica FDS Server has been able to reconnect to master FDS Server, it clears the alarm.		
Remedial action: 1. Check that the node where the master FDS Server should be running has started properly. \n\n2. Check also that the connection between the nodes is ok and that the replica in question has been configured in master's start-up parameters. \n\nIf these actions do not work, contact your local Nokia representative and provide them with information from the information fields of the alarm.		

Table 41-69 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 41-70 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 41-71 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 41-72 CORRUPTED_ALARM_DATA

Alarm	Attributes	Applicable major release
Name: CORRUPTED_ALARM_DATA (11660) Type: processingErrorAlarm Package: racloms.CORRUPTED_ALARM_DATA Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CORRUPTED ALARM DATA Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: CORRUPTED ALARM DATA\n\nCorrupted data found in the alarm log file.\n\nThe corrupted record in the alarm log file is ignored, meaning that it is possible that an alarm notification was lost or a more serious system error has occurred.\n\nClear the alarm with alarm management application after correcting the fault as presented in INSTRUCTIONS.		
Remedial action: 1. Fill in a problem report with the alarm data and send it to your local Nokia representative.		

Table 41-73 CORRUPTED_LDAP_DATABASE_RECOVERED

Alarm	Attributes	Applicable major release
Name: CORRUPTED_LDAP_DATABASE_ RECOVERED (11661) Type: processingErrorAlarm Package: racloms.CORRUPTED_LDAP_DATABASE_ RECOVERED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CORRUPTED LDAP DATABASE RECOVERED Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: CORRUPTED LDAP DATABASE RECOVERED\n\nA primary or secondary LDAP (Lightweight Database Access Protocol) database was corrupted but it has been successfully recovered. The LDAP databases can get corrupted, for example, when\n- a disk becomes full while the database is being updated\n- a node failure and/or ungraceful node restart happens while the database is being updated.\n\nThe platform software has automatically recovered the database from an operational primary or secondary database. Some applications may have been impacted by the temporary unavailability of the LDAP database. As the platform restarts the failed applications, the problem should not have caused permanent problems.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This is an informative alarm. No operator actions required.		

Table 41-74 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • LOMS16A
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 41-75 CPU_MALFUNCTION

Alarm	Attributes	Applicable major release
Name: CPU_MALFUNCTION (11662) Type: equipmentAlarm Package: racloms.CPU_MALFUNCTION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CPU MALFUNCTION Implicitly cleared: false Default probable cause: PROCESSOR_PROBLEM_M3100	Release: • LOMS16A
Description: CPU MALFUNCTION\n\nA problem in the central processing unit (CPU) functionality has been detected.\n\nPossible error types are:\n\nIERR (internal error)\nThermal Trip\nFRB1/BIST (fault resilient boot/built-in self-test) failure\nFRB2/Hang in POST (power-on self-test) failure (believed to be due to a\nprocess failure or related to a processor failure)\nFRB3/Processor Startup/Initialization failure (CPU didn't start)\nConfiguration Error\nSM BIOS (system management basic input/output system) 'Uncorrectable CPU-complex\nError'\nProcessor Presence not detected\nProcessor disabled\nTerminator Presence Detected\n\nThe CPU may be out of service.\n\nClear the alarm after correcting the fault, according to the instructions provided.		
Remedial action: 1. Check that the affected unit is healthy, and is plugged-in properly.\n\n2. Restart the unit, if necessary.\n\n3. Replace the unit, if necessary.\n\n4. If the problem exists even after following these instructions, please contact your local Nokia representative.		

Table 41-76 CPU_USAGE_OVER_LIMIT

Alarm	Attributes	Applicable major release
Name: CPU_USAGE_OVER_LIMIT (11663) Type: qualityOfServiceAlarm Package: racloms.CPU_USAGE_OVER_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CPU USAGE OVER LIMIT Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A

Table 41-76 CPU_USAGE_OVER_LIMIT (continued)

Alarm	Attributes	Applicable major release
Description: CPU USAGE OVER LIMIT\n\nA processor is being used at a very high throughput level because the execution of some processes takes a lot of CPU time.\n\nThere is a risk that the node is unable to fulfil the tasks allocated to it. This depends on to what extent certain processes are taking the most of the CPU time and blocking other processes from getting runtime on the CPU, and whether there is a temporary or a permanent increase on the throughput.\n\nIf the processor is constantly used at a very high throughput level, the system might appear very slow. For example, the execution of commands takes a long time to finish.\n\nDo not clear the alarm. The alarm is cleared automatically by the fault detector of the operating system when CPU usage is on a low enough level. The raising or clearing thresholds are different to prevent unnecessary trashing.		
Remedial action: 1. Run "top" Linux command on the node that reports the alarm. The command gives a repetitive update of processor activity in real time. It gives a listing of the most CPU-intensive tasks of the system.\n\n2. If the problem persists, contact your Nokia representative and provide the information gathered in the previous step.		

Table 41-77 CRL_DOWNLOAD_FAILURE

Alarm	Attributes	Applicable major release
Name: CRL_DOWNLOAD_FAILURE (11664) Type: communicationsAlarm Package: racloms.CRL_DOWNLOAD_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CRL DOWNLOAD FAILURE Implicitly cleared: false Default probable cause: TRANSMISSION_ERROR	Release: • LOMS16A
Description: CRL DOWNLOAD FAILURE\n\nDownload of valid CRL for peer certificate from CRL Distribution Point has failed\n\nThe alarm is raised when OMS Platform fails to retrieve or validate a Certificate Revocation List for peer certificate from the server\n\nClear the alarm with the alarm management application after checking correctness of URL for CRL distribution point server, connectivity to the server or validity of signature for related CRL		
Remedial action: Depending on the reason information perform one of the following checks:\n\n1. Verify URL of CRL distribution point server in certificate extension. If URL stored in certificate extension is correct, then connectivity to the CRL distribution point server should be also checked.\n\n2. Verify URL of CRL distribution point server in certificate extension. If URL stored in certificate extension is correct, then check LDAP configuration on CMP server.\n\n3. Verify signature of CRL available at indicated URL.		

Table 41-78 CRL_UPDATE_FAILURE

Alarm	Attributes	Applicable major release
Name: CRL_UPDATE_FAILURE (11665) Type: communicationsAlarm Package: racloms.CRL_UPDATE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CRL UPDATE FAILURE Implicitly cleared: true Default probable cause: TRANSMISSION_ERROR	Release: • LOMS16A
Description: CRL UPDATE FAILURE\n\nThe alarm is raised when the OMS fails to retrieve or validate a Certificate Revocation List from the server.\n\nThe alarm may have effect on the OMS security. If the certificate revocation list (CRL) cannot be updated it is not possible to validate used certificates against CRL.\n\nThe alarm is cleared automatically by the alarm system after NE can reach CR server.		

Table 41-78 CRL_UPDATE_FAILURE (continued)

Alarm	Attributes	Applicable major release
Remedial action: Depending on the reason information perform one of the following checks:\n\n1. Verify CMP server parameters in OMS LDAP. If parameters stored in LDAP are correct, then connectivity to the CRL distribution point server should be also checked.\n2. Verify CMP server parameters in OMS LDAP. If parameters stored in LDAP are correct, then check LDAP configuration on CMP server.\n3. Verify size and signature of CRL available at indicated CR server.\n4. Verify if DP (Distribution Point) for cert xx is defined, or check CRL client configuration for DP retrieval.\n\nWhen the above mentioned steps have been done, the CRL update operation should be repeated.		

Table 41-79 CURRENT_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: CURRENT_OUT_OF_LIMIT (11666) Type: equipmentAlarm Package: racloms.CURRENT_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: CURRENT OUT OF LIMIT Implicitly cleared: false Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: CURRENT OUT OF LIMIT\n\nThe unit's current has exceeded the programmed threshold.\n\nThe unit may behave erratically.\n\nClear the alarm after correcting the fault, according to the instructions provided.		
Remedial action: 1. Check the power feed in the cabinet for proper input current.\n\n2. Check that the affected unit is healthy, and is plugged-in properly.\n\n3. Restart the unit, if necessary.\n\n4. Replace the unit, if necessary.\n\n5. If the problem exists even after following these instructions, please contact your local customer support.		

Table 41-80 DIAMETER_BASE_PROTOCOL_CONFIGURATION_FAILURE

Alarm	Attributes	Applicable major release
Name: DIAMETER_BASE_PROTOCOL_ CONFIGURATION_FAILURE (11667) Type: processingErrorAlarm Package: racloms.DIAMETER_BASE_PROTOCOL_ CONFIGURATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: DIAMETER BASE PROTOCOL CONFIGURATION FAILURE Implicitly cleared: false Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A
Description: DIAMETER BASE PROTOCOL CONFIGURATION FAILURE\n\nThe Diameter base protocol configuration has failed due to the invalid Diameter base protocol configuration data in the lightweight directory access protocol (LDAP). One of the mandatory fields or its value is missing.\n\nThe Diameter service is unavailable. The Diameter service cannot be used by the applications until the configuration has been corrected.\n\nClear the alarm with Alarm Browser after correcting the fault as presented in Instructions.		

Table 41-80 DIAMETER_BASE_PROTOCOL_CONFIGURATION_FAILURE (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the Application Additional Info field to find out the mandatory field that has been incorrectly configured in the Diameter base protocol LDAP configuration data. \n\nCorrect the configuration data (see the error lists below) and restart the application. \n\nFor further details on the problem, see the error logs in syslog. \nIf the configuration is correct, contact your local Nokia Customer Service Center. \n\nThe Diameter application defines the location of the Diameter base protocol configuration in the LDAP. The exact location is described in the configuration instructions of the application. For more information how to browse and modify the LDAP objects or attributes, see Parameter Management customer documentation.\n\nIf the Additional Info can be found in the following list, the corresponding entry is missing from the Diameter base protocol LDAP configuration:\n\nMAIN_CONFIG_DOES_NOT_EXIST: fsdiaMainConfiguration\nPEERTABLE_CONF_DOES_NOT_EXIST: fsdiaPeerTableConfiguration\nREALMTABLE_CONF_DOES_NOT_EXIST:fsdiaRealmTableConfiguration\nPEERRECORD_MISSING: fsdiaPeerRecord\nREALMRECORD_MISSING: fsdiaRealmRecord\nSCTP_CONFIG_MISSING:fsdiaSctpConfig\nINVALID_SCTP_PORT: fsdiaSctpPortEntry\nSCTP_FQDN_MISSING: fsdiaSctpFqdnEntry \nTCP_CONFIG_MISSING: fsdiaTcpConfig\nTCP_FQDN_MISSING: fsdiaTcpFqdnEntry\nINVALID_TCP_PORT: fsdiaTcpPortEntry \n\nIf Additional Info can be found in the following list, the corresponding attribute is missing from the Diameter base protocol LDAP configuration:\n\nDIAMETER_ID_MISSING: fsdiaDiameterId in entry fsdiaPeerRecord\nACTION_MISSING: fsdiaAction in entry fsdiaRealmRecord\nAPPLICATION_ID_MISSING: fsdiaApplicationId in entry fsdiaRealmRecord \nREALM_NAME_MISSING: fsdiaRealmName in entry fsdiaRealmRecord\nORIGIN_REALM_MISSING: fsdiaOriginRealm in entry fsdiaMainConfiguration\nPRODUCT_NAME_MISSING: fsdiaProductName in entry fsdiaMainConfiguration\nVENDOR_ID_MISSING: fsdiaVendorId in entry fsdiaMainConfiguration\nINVALID_SCTP_FQDN: fsdiaSctpFqdn in entry fsdiaSctpFqdnEntry \nINVALID_TCP_FQDN: fsdiaTcpFqdn in entry fsdiaTcpFqdnEntry\n\nOther errors:\nCONFIGURATION_PARSING_FAILED: The logging facility is incorrectly initialized. Fill in a problem report and send it to your local Nokia Customer Service Center. Include in the Problem Report the error logs from syslog.\nINCORRECT_PATH: \nThe path for retrieving the Diameter configuration parameters is incorrectly set by the Diameter application. Fill in a problem report and send it to your local Nokia Customer Service Center. Include in the problem report the error logs from the syslog.\nREALMTABLE_CONFIGURATION_PARSING_FAILED:\nAn unexpected error occurred when parsing configuration in fsdiaRealmTableConfiguration="realmTable entry. Check and correct the realmTable configuration.\nGETHOSTNAME_ERROR\nConstructing the default value for the parameter fsdiaOriginHost in entry fsdiaMainConfiguration=mainConfiguration has failed. Add a value to the parameter."		

Table 41-81 DISK_DATABASE_IS_GETTING_FULL

Alarm	Attributes	Applicable major release
Name: DISK_DATABASE_IS_GETTING_FULL (11668) Type: processingErrorAlarm Package: racloms.DISK_DATABASE_IS_GETTING_FULL Raised on class: racloms.OMS	Severity: indeterminate Specific problem: DISK DATABASE IS GETTING FULL Implicitly cleared: true Default probable cause: STORAGE_CAPACITY_PROBLEM_M3100	Release: • LOMS16A
Description: DISK DATABASE IS GETTING FULL\n\nThe disk storage area reserved for disk database is filling up.\n\nThe disk database is still fully operational. If the database fills up completely, its services cannot be used anymore.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: The actions to be done in order to avoid a completely full database are database-specific, so contact your local Nokia representative immediately and provide them with the information you obtained from the alarm notification's fields.		

Table 41-82 DISK_DATABASE_WATCHDOG_START_UP_FAILED

Alarm	Attributes	Applicable major release
Name: DISK_DATABASE_WATCHDOG_START_UP_FAILED (11669) Type: processingErrorAlarm Package: racloms.DISK_DATABASE_WATCHDOG_START_UP_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: DISK DATABASE WATCHDOG START-UP FAILED Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: DISK DATABASE WATCHDOG START-UP FAILED\n\nStart-up of the disk database watchdog has failed due to a configuration error, or\nother reasons.\n\nBecause the disk database and its watchdog belong to the same recovery unit (RU), the disk database watchdog start-up failure means that the database is not available.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check the Application Additional Information field for a reason for the configuration error: \n\nReason 1: Disk database watchdog failed to read the parameters from parameter management\nReason 2: Invalid or missing parameter value\n\nand continue according to the following procedure:\n\n1. Check that the following parameters exist in parameter management for each database entry in the database fragment with the DN (Distinguished Name) "fsFragmentId="DB, fsClusterId=ClusterRoot":\nfsdbRedundancyModel\nfsdbDataSourceName\nfsdbFillRatioAlarmLimit\nfsdbFillRatioCheckFreq\n2. Use Parameter Tool to get the values of those parameters for the database in question. To find the the parameters, use the value of the Managed Object -field in the alarm management application, for example:\nfsdbName=DB_Alarm,fsFragmentId=DB,fsClusterId=ClusterRoot\n3. Send the values found and/or parameters that do not exist to your Nokia representative."		

Table 41-83 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • LOMS16A
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 41-84 DRBD_HARDWARE_FAILURE

Alarm	Attributes	Applicable major release
Name: DRBD_HARDWARE_FAILURE (11670) Type: equipmentAlarm Package: racloms.DRBD_HARDWARE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: DRBD HARDWARE FAILURE Implicitly cleared: false Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A

Table 41-84 DRBD_HARDWARE_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: DRBD HARDWARE FAILURE\n\nA physical disk partition of a Distributed Replicated Block Device (DRBD) is broken or is reporting errors. \nDRBD is used to replicate data of an application partition between two nodes. The nodes form an active/standby redundancy pair where a standby node can take over in case the active node or application fails. \nThe identified DRBD partition or logical volume is currently unavailable or functioning poorly.\n\nThe service that the application provides is not impacted if the other node and the DRBD device are still functioning. In this case, the application is however no longer redundant, and recovery from possible forthcoming failures may take longer or may not be possible at all. \nThe service provided by the application is down if also the other node or partition is not functioning.\n\nClear the alarm manually after the disk has been replaced.		
Remedial action: This situation is most likely caused by a hardware fault. Contact your Nokia representative to have the disk replaced.		

Table 41-85 DRBD_SYNCHRONIZATION_FAILURE

Alarm	Attributes	Applicable major release
Name: DRBD_SYNCHRONIZATION_FAILURE (11671) Type: qualityOfServiceAlarm Package: racloms.DRBD_SYNCHRONIZATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: DRBD SYNCHRONIZATION FAILURE Implicitly cleared: true Default probable cause: SYSTEM_RESOURCES_OVERLOAD	Release: • LOMS16A
Description: DRBD SYNCHRONIZATION FAILURE\n\nA secondary Distributed Replicated Block Device (DRBD) does not synchronise or synchronises very slowly with the primary DRBD device. \nDRBD is used to replicate data of an application partition between two nodes. The nodes form an active/standby redundancy pair where a standby node can take over in case the active node or application fails. When the two disk images are not identical (for example, following a node reboot) they are synchronised by copying the changed data from the primary DRBD to the secondary DRBD. \nCurrently synchronisation to the identified secondary DRBD partition or logical volume is not proceeding or proceeds extremely slowly.\n\nIf the node running the primary DRBD (and the application) is functioning, there is no immediate impact to the service that the application provides. The identified DRBD partition or logical volume is, however, not currently available as a backup resource. Any failure in the node that currently runs the application causes a long or permanent service interruption.\nThe service is down if the node with the primary DRBD is not functioning.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This situation can be caused by a node or network overload. Contact your Nokia representative to get assistance in the analysis.		

Table 41-86 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		

Table 41-86 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 41-87 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 41-88 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • LOMS16A
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 41-89 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		

Table 41-89 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 41-90 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • LOMS16A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 41-91 ETHERNET_INTERFACE_USAGE_OVER_LIMIT

Alarm	Attributes	Applicable major release
Name: ETHERNET_INTERFACE_USAGE_OVER_LIMIT (11672) Type: qualityOfServiceAlarm Package: racloms.ETHERNET_INTERFACE_USAGE_OVER_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ETHERNET INTERFACE USAGE OVER LIMIT Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: ETHERNET INTERFACE USAGE OVER LIMIT\n\nThe Ethernet interface is used at a very high level. This alarm may be raised, for example, when large files are copied over the network causing a lot of network file system (NFS) traffic.\n\nPackages are not lost yet but if the interface is loaded increasingly, packages might eventually be lost.\n\nDo not clear the alarm. The alarm is automatically cleared by the operating system's fault detector once the Ethernet load has decreased to a tolerable level.		
Remedial action: This is an informative alarm and does not require direct actions.		

Table 41-92 ETHERNET_LINK_FAILURE

Alarm	Attributes	Applicable major release
Name: ETHERNET_LINK_FAILURE (11673) Type: equipmentAlarm Package: racloms.ETHERNET_LINK_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ETHERNET LINK FAILURE Implicitly cleared: true Default probable cause: LINK_FAILURE	Release: • LOMS16A
Description: ETHERNET LINK FAILURE\n\nThe redundancy of Ethernet is lost because of an Ethernet link failure. The error might have been caused by a hardware failure. It can either be a broken Ethernet port by an unplugged cable on the front panel of the gateway (GW) node, or if some program or user issued a command shutting down the Ethernet interface.\n\nIn case of a subsequent link failure, Ethernet packages are lost. This means that the node cannot receive or transmit data over the network.\n\nThe alarm is automatically cleared by the operating system's fault detector when the Ethernet link comes up. If raised due to unused Ethernet interfaces, the alarm is cleared as soon as the admin state of those interfaces is set to DOWN.		
Remedial action: 1. If the alarm is raised for an external Ethernet interface, check that the cable is properly connected on the front panel of the GW node.\n\n2. Take a console connection to the node with the alarming interface.\n\n3. Check the status of the interface with the following command: \n\nifconfig -a <interface> \n\nFor example, ifconfig -a eth0\n\n4. Assuming that the interface does not have the UP and RUNNING flags set, try to configure the interface UP with the following command: \n\nifup <interface>\n\nFor example, ifup eth0\n\n5. For every single Ethernet link interface, an Alarm 70164 is raised even for those that are not connected. To suppress such alarms, the port admin state of unused interfaces should be 'DOWN'.\n\n6. If the environment is a box controller node (BCN) with less than 6 box setup, alarms will be raised. To suppress these alarms, the port admin state should be set to 'DOWN' in all local management processors (LMPs).\n\n- If a user adds/removes BCNs to the existing BCN setup (dynamically) and the total number of BCN boxes is still less than 6, then the user should change the port admin state to 'DOWN' for suppressing these alarms. \n\n- If a user adds new BCNs to the existing BCN setup (dynamically) and the total number of BCN boxes are 6, then the user should change the port admin state to 'UP' for all existing BCNs boxes to trigger back the alarms.\n \nThe following SCLI commands can be used for making SwitchPortAdminState UP/DOWN\n\nFor example, set config-mode on\n set config attribute fsClusterId="ClusterRoot fsFragmentId=HA \n fsFragmentId=LMP fsipHostName=LMP-x-x-x fsFragmentId=Switch \n fsipSwitchPortName=xxxx attribute-list fsipSwitchPortAdminState up/down\n set config-mode off\n\n7. If the above steps cannot resolve the situation, contact your local customer support.\n\nNote: In a deployment where not all external interfaces are used, a number of alarms equal to the number of unused Ethernet links will be raised. To avoid getting those deceptive alarms (since they are actually the result of unused links and not of failing links), the operator is advised to set the admin state of all unused links DOWN using the following SCLI command:\n\nset networking interface iface <iface-name> admin down"		

Table 41-93 EXCESSIVE_NUMBER_OF_IPMI_EVENTS

Alarm	Attributes	Applicable major release
Name: EXCESSIVE_NUMBER_OF_IPMI_EVENTS (11674) Type: equipmentAlarm Package: racloms.EXCESSIVE_NUMBER_OF_IPMI_EVENTS Raised on class: racloms.OMS	Severity: indeterminate Specific problem: EXCESSIVE NUMBER OF IPMI EVENTS Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: EXCESSIVE NUMBER OF IPMI EVENTS\n\nThe limit of the number of events from a single chassis in a specified time window has been exceeded. The event adapter discards events until the number of the events in the time window falls below the limit.\n\nWhen the alarm is active, the IPMI (Intelligent Platform Management Interface) event adapter discards all events. After the alarm has been cancelled, the alarm database may not correspond to the actual alarm state.\nNote that some IPMI events may have been lost due to the incident.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: If the alarm is not cleared automatically, contact your local Nokia representative.		

Table 41-94 EXTERNAL_ETHERNET_SWITCH_CONNECTION_FAILURE

Alarm	Attributes	Applicable major release
Name: EXTERNAL_ETHERNET_SWITCH_ CONNECTION_FAILURE (11675) Type: communicationsAlarm Package: racloms.EXTERNAL_ETHERNET_ SWITCH_CONNECTION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: EXTERNAL ETHERNET SWITCH CONNECTION FAILURE Implicitly cleared: true Default probable cause: LAN_ERROR	Release: • LOMS16A
Description: EXTERNAL ETHERNET SWITCH CONNECTION FAILURE\n\nThe LAN (Local Area Network) monitoring software has detected a fault in all the interfaces connecting to the same external Ethernet switch.\n\nThis is a serious condition as the redundancy level of the system is lowered due to the failed switch. All traffic going through the external network can be disrupted. The user is required to check the state of the external network components immediately.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check the severity of the alarm. \nIf the severity is WARNING, then:\nThe system is trying to recover the interfaces connecting to the switch: no actions are needed at this point.\nIf the severity is MAJOR, then:\nIf the "are_resets_enabled" parameter is true in the alarm info, the system has already tried to reset the interfaces connecting to the switch and the method of repairing the fault is to replace the switch.\nIf "are_resets_enabled" is off, however, it means that no automatic resets have been executed and manual reset could be beneficial as detailed in the hardware maintenance documentation.\nThe name of the switch is included in the application additional info. As the switch is external, its 'location' cannot be specified. The interfaces connecting to the switch are configured into the LDAP beforehand as part of the deployment.\nRefer to the hardware maintenance documentation for how to change a faulty switch. After replacing the switch and powering it on or restarting it, allow the system at least five (5) minutes to stabilise the fault information. During that time other alarms might appear and this alarm might be cancelled for a while but do not react to the other alarms.		

Table 41-95 EXTERNAL_LDAP_FAILURE

Alarm	Attributes	Applicable major release
Name: EXTERNAL_LDAP_FAILURE (11676) Type: processingErrorAlarm Package: racloms.EXTERNAL_LDAP_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: EXTERNAL LDAP FAILURE Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_ UNAVAILABLE	Release: • LOMS16A

Table 41-95 EXTERNAL_LDAP_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: EXTERNAL LDAP FAILURE\n\nA network element (NE) experiences problems with the connection to the NetAct external Lightweight Directory Access Protocol (LDAP) server.\nThe alarm is raised for the following types of problems:\n1. Both primary and secondary NetAct LDAP servers are down, unreachable, not responding within certain time, or replying with a return code indicating that LDAP is busy. This indicates a failure.\n2. The NE account is not accepted by neither the primary nor the secondary NetAct LDAP servers. This case affects the long-term functionality. Note that if the NE is configured to fallback to the initial registration account if the NE account is invalid, an alarm in this case does not indicate inability of the NE to use NetAct LDAP, because initial registration account is used temporarily. \n3. Both the NE account and the initial registration account are not accepted by neither the primary nor the secondary NetAct LDAP servers. This indicates a failure.\n4. Bad LDAP data (for example, loops in referrals, too big a result set).\n5. Other type of problem, for example invalid RUIM configuration in the local LDAP server.\n\nThe NE is trying to contact the external NetAct LDAP server in the following scenarios:\n1. NE connects to the NetAct LDAP server to verify the password information of the external user.\n2. NE connects to the NetAct LDAP server to obtain the authorisation data of the external user. There are several use cases when this scenario is triggered:\na. User authorisation data is fetched and replicated locally during the first login of an external user into the NE or a login occuring after the replicated user account is removed from NE internal user database due to cache expiry. This scenario occurs after external user's password has been verified in the context of user authentication.\nb. User authorisation data replication triggered by NE Name Service Switch (NSS) module, for example, by using id command.\nc. User authorisation data is fetched and replicated after a Command Line Interface (CLI) command using fsruimrepcli tool is issued. Please see user manual page for fsruimrepcli for details.\nd. User authorsation data is fetched and replicated due to a scheduled cache update. Scheduled cache updates are performed by RuimReplicator process of the RuimRep Recovery Group automatically and regularly with time interval in between replications as configured by the following property in RuimReplicator property file (in /opt/Nokia_BP/SS_AAA/etc/):\n// automatic cache refresh interval in seconds\nruim.replicator.refresh_interval\n\nProblem 2 does not prevent any scenario from successful completion. If this problem occurs, an alarm is raised.\nProblems 1 and 3 prevent successful completion of all scenarios and effect of those problems is described below:\nIn scenarios 1 and 2a, external user's login is denied with the appropriate PAM (Pluggable Authentication Module) error code. \nIn scenario 2b, there can be various problems related to user-to-group mappings for external users. \nIn scenario 2c, no alarm is raised (CLI).\nIn scenario 2d RuimReplicator process of the RuimRep Recovery Group performs time-based replication automatically and regularly with time interval in between replications as configured by the following property in RuimReplicator property file (in /opt/Nokia_BP/SS_AAA/etc/):\n// automatic cache refresh interval in seconds\nruim.replicator.refresh_interval\n\nIf the time-based replication fails due to the NetAct LDAP server unavailability (problem 1), RuimReplicator process starts to recover from the failure by retrying the replication according to the following properties:\n// retry count incase of cache refresh failure\nruim.replicator.refresh_retry_count\n\n// sleep between cache refresh tries in seconds\nruim.replicator.refresh_retry_interval\n\nIf LDAP server is still not available after ruim.replicator.refresh_retry_count retries, RuimReplicator switches to the secondary NetAct LDAP server. An alarm is raised if the secondary NetAct LDAP server is not available either.\nIn case of problems 2 and 3, during time-based replication, RuimReplicator raises an alarm without retrying.\nWhile RuimReplicator is experiencing problems with external LDAP it is possible that there were access control changes made in NetAct, which are not propagated to the NE. If there are users logged in, for example, the sessions still operate with permissions based on the last successfully replicated data.\n\nAlarm is automatically cleared by the RuimReplicator when replication is successful. The alarm is also cleared when a new alarm with the same specific problem but with different Identifying Application Additional Info is raised by the RuimReplicator.		
Remedial action: Depending on the problem type (see Identifying Application Additional Info) the cause for the problem can be:\n- Network configuration problems. Check that the primary and secondary NetAct LDAP server addresses defined in the active configuration fragment under NWI3 Mediator fragment in internal LDAP server (fsFragmentId="mediator,fsFragmentId=NWI3, fsClusterId=ClusterRoot) are reachable with the ping command.\n- NE account expired or deleted in NetAct. Check that the NE account stored in the internal LDAP server in the NWI3 security fragment configuration in LDAP (fsFragmentId=security, fsFragmentId=NWI3, fsClusterId=ClusterRoot) exists also in the primary NetAct LDAP servers and has not expired.\n- NetAct generated a new NE account, but the NE did not receive it. Check that the NE account username and password stored in the NE's internal LDAP fragment (fsFragmentId=security, fsFragmentId=NWI3,fsClusterId=ClusterRoot) are the same as the ones stored in the NetAct LDAP server.\n- NetAct LDAP is overloaded or shut down."		

Table 41-96 EXTERNAL_STORAGE_SYSTEM_FAILURE

Alarm	Attributes	Applicable major release
Name: EXTERNAL_STORAGE_SYSTEM_FAILURE (11677) Type: equipmentAlarm Package: racloms.EXTERNAL_STORAGE_SYSTEM_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: EXTERNAL STORAGE SYSTEM FAILURE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: EXTERNAL STORAGE SYSTEM FAILURE\n\nFailure in the external storage system has been detected.\n\nThe external storage system is behaving erratically, is non-responsive, or becomes non-responsive if this error is not solved. More details can be found in the eventText description of the Application Additional Info field.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. For instructions, check the manufacturer's documentation for EMC CLARiiON storage system.\n2. If the problem remains, contact your local Nokia representative to replace the external storage unit. \nCaution: Risk of data loss. Before replacing an operational disk drive, take the\nnecessary backups.\nYou can find the details of the faulty storage unit in the Identifying Application Additional Info field and Application Additional Info field of the alarm.		

Table 41-97 EXTERNAL_USER_ACCOUNT_VALIDATION_FAILED

Alarm	Attributes	Applicable major release
Name: EXTERNAL_USER_ACCOUNT_VALIDATION_FAILED (11678) Type: processingErrorAlarm Package: racloms.EXTERNAL_USER_ACCOUNT_VALIDATION_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: EXTERNAL USER ACCOUNT VALIDATION FAILED Implicitly cleared: false Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: EXTERNAL USER ACCOUNT VALIDATION FAILED\n\nNetwork element (NE) has detected that according to the NetAct Remote User Information Management (RUIM) LDAP (Lightweight Directory Access Protocol) access control lists, an external user account defined in NetAct LDAP user database has permissions for this NE. According to the NE security architecture, remote user accounts are replicated locally. The validation check performed before the replication for the user account did not pass and therefore the user account was not replicated. \nPossible reasons for a failing validation check are:\n1. External username is the same as one of the NE internal usernames. This should not happen if NetAct is following the agreed way of naming users.\n2. External username is a reserved username. \n3. External username is invalid, for example, too long (supported usernames are up to 31 characters long).\n4. External username contains invalid characters.\n5. Account is not assigned with any valid permissions.\n6. External user ID is the same as one of internal user IDs.\n7. External user ID is not in the supported range.\n8. Some permissions do not map to any valid groups.\n9. User ID is not a valid number.\n\nThe user account cannot be used to log into the NE (except for case 8 above, where user is still able to log in).\n\nClear the alarm with an alarm management application after correcting the fault as presented in Instructions.		
Remedial action: Check that the username complies with the restrictions imposed by the NE and correct the account information in NetAct LDAP.\nThe restrictions (based on /RUIMFLEXI/) are the following:\n- the username must be created according to [a-zA-Z0-9_.][a-zA-Z0-9_-.]{0,30}{a-zA-Z0-9_.$-]? (32 characters maximum)\n- the username cannot start with one of the prefixes reserved for network elements: "_nok", "_nsn"\n- the username cannot be the same as one of the reserved names from the list (defined in /RUIMFLEXI/): root, wheel, daemon, adm, sync, shutdown, halt, lp, mail, uucp, operator, games, nobody, gopher, nfs, nfsnobody, named, ntp, ldap, mysql, postgres, apache, sshd, rpm, dbus, vcsa, nscd\n- the numeric user ID of a RUIM user must be in the range of [1.000, 9.999.999], that is, greater or equal to one thousand and less than ten million.\n- the account must be assigned with at least one valid permission. Valid permissions are those that allow mapping an external user account to one or more network element groups.		

Table 41-98 FailedStatsCollectionAtAcknowledge

Alarm	Attributes	Applicable major release
Name: FailedStatsCollectionAtAcknowledge (11695) Type: communicationsAlarm Package: racloms. FailedStatsCollectionAtAcknowledge Raised on class: racloms.OMS	Severity: major Specific problem: PM Collection Issue while acknowledging PM files Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LOMS16A
Description: PM Collection Issue while acknowledging PM files\nThe alarm will be cleared automatically at the next successful request.		
Remedial action: Please refer to the LTE Nokia Node Maintenance manual for remedial action information.		

Table 41-99 FailedStatsProcessing

Alarm	Attributes	Applicable major release
Name: FailedStatsProcessing (11696) Type: processingErrorAlarm Package: racloms.FailedStatsProcessing Raised on class: racloms.OMS	Severity: minor Specific problem: PM Collection Issue while processing PM files Implicitly cleared: true Default probable cause: corruptData	Release: • LOMS16A
Description: PM Collection Issue while converting PM files\nThe alarm will be cleared automatically at the next convertion period.		
Remedial action: Please refer to the LTE Nokia Node Maintenance manual for remedial action information.		

Table 41-100 FAILED_TO_CREATE_NETACT_CONNECTION

Alarm	Attributes	Applicable major release
Name: FAILED_TO_CREATE_NETACT_ CONNECTION (11679) Type: communicationsAlarm Package: racloms.FAILED_TO_CREATE_NETACT_ CONNECTION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FAILED TO CREATE NETACT CONNECTION Implicitly cleared: true Default probable cause: CALL_ESTABLISHMENT_ ERROR	Release: • LOMS16A
Description: FAILED TO CREATE NETACT CONNECTION\n\nThe NWI3 adapter failed to register to Nokia NetActTM.\n\nNetAct cannot subscribe to notifications or be used for managing the network element via network interface 3 (NWI3).\n\nThe alarm is cleared once NetAct has connected to OMS, and NWI3Adapter\nhas successfully re-registered itself to NetAct at the specified time interval.\n\nIf the connection between NetAct and OMS has been successfully established, but NWI3Adapter is not re-registered with NetAct, the alarm will remain active until the next attempt for re-registration is successful (after the specified time interval; approximately 15+ minutes). \n\nBut between the time that the alarm is active, NetAct can still perform some operations like alarm upload and CM, because it is physically connected with the OMS and contains the IOR of the NWI3Adapter's session manager. \n\nUsing this IOR, NetAct can trigger some operations with NWI3Adapter, though logically both NWi3Adapter and NetAct are not connected.		

Table 41-100 FAILED_TO_CREATE_NETACT_CONNECTION (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. If file /var/opt/Nokia/SS_Nwi3Adapter/config/nwi3mdcorba.ini exists:\na) Make sure that the NetAct Registration Service IOR (parameter registrationServiceIOR) is filled and check the correctness of the interoperable object reference (IOR). The command printIOR can be used for viewing the IP address and port included in the IOR.\nb) Verify that there is a valid username (parameter registrationServiceUsername) and password (registrationServicePassword) to the registration service of NetAct in file /var/opt/Nokia/SS_Nwi3Adapter/config/nwi3mdcorba.ini.\nc) Check the value of the takeIntoUseNext parameter in the nwi3mdcorba.ini file. The value of the parameter in an active section should be 1, and the value of the configurationActive parameter should also be 1. The system sets the value of the configurationActive parameter automatically to 1 when a parameter set is used.\n\n2. If file /var/opt/Nokia/SS_Nwi3Adapter/config/nwi3mdcorba.ini does not\nexist and NWI3 adapter's configuration is stored under branch fsFragmentId="mediator, fsFragmentId=NWI3, and fsClusterId=ClusterRoot in the LDAP:\na) Verify that there is an LDAP entry fsnwi3N3CFId=<id>, fsFragmentId=mediator, and fsFragmentId=NWI3 with attribute fsnwi3takeIntoUseNext=true, which defines the active attribute set.\nb) Make sure that the NetAct Registration Service IOR (attribute fsnwi3registrationServiceIOR) has been specified for the active set and check the correctness of the IOR. Command printIOR can be used for viewing the IP address and port included in the IOR.\nc) If attributes fsnwi3NEAccountUsername and fsnwi3NEAccountPassword exist under branch fsFragmentId=security and fsFragmentId=NWI3, they are used for NetAct registration. Verify that both are valid.\nd) If attributes fsnwi3NEAccountUsername and fsnwi3NEAccountPassword do not exist under branch fsFragmentId=security and fsFragmentId=NWI3, the initial username (attribute fsnwi3initialRegistrationUsername) and password (fsnwi3initialRegistrationPassword) defined in the active set are used for NetAct registration. Verify that both are valid.\n3. Verify that NetAct is up and running and check the connection between\nthe network element and NetAct. \n4. Check that the NetAct host name is configured to the external DNS in\nuse."		

Table 41-101 FALLBACK_OCCURED

Alarm	Attributes	Applicable major release
Name: FALLBACK_OCCURED (11680) Type: processingErrorAlarm Package: racloms.FALLBACK_OCCURED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FALLBACK OCCURED Implicitly cleared: false Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A
Description: FALLBACK OCCURED\n\nThe alarm is raised if there are errors during a major software upgrade (MSU) procedure, which will prevent the new version of FlexiPlatform from running after an upgrade. If this alarm is raised, it means either there were errors during the boot of the new FlexiPlatform-based system or during the last configuration steps of an application.\n\nThis alarm is raised when errors prevented the MSU procedure from being executed. If this alarm is active, it means that the old installation is still running.\n\nAfter correcting the fault, clear the alarm with an alarm management application.		
Remedial action: Fill in a problem report and send it to your local Nokia representative. The operator should verify the msu.log and check the cause of the MSU error.		

Table 41-102 FAST_DATA_STRUCTURE_AUTOMATIC_RECOVERY_FAILED

Alarm	Attributes	Applicable major release
Name: FAST_DATA_STRUCTURE_AUTOMATIC_RECOVERY_FAILED (11681) Type: processingErrorAlarm Package: racloms.FAST_DATA_STRUCTURE_AUTOMATIC_RECOVERY_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FAST DATA STRUCTURE AUTOMATIC RECOVERY FAILED Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A

Table 41-102 FAST_DATA_STRUCTURE_AUTOMATIC_RECOVERY_FAILED (continued)

Alarm	Attributes	Applicable major release
Description: FAST DATA STRUCTURE AUTOMATIC RECOVERY FAILED\n\nA fast data structure (FDS) server was coming up and loading the data structure to memory, but a checkpoint file and/or log file was corrupted.\n\nThe FDS does not start, and client applications cannot access it. In addition, the data of the FDS may be lost.\n\nThe alarm is cleared once the fault in question has been repaired.\n\nIn this case, the application raises an alarm and then restarts, as it cannot function with the fault in question. Due to its restart, the alarm system assumes that the alarm is obsolete and clears it immediately. This process continues till the defect that caused the alarm has been removed.		
Remedial action: 1. If the role of the FDS is MASTER and the application that uses the FDS is not capable of re-creating the FDS contents, restore the datastore from the latest backup.\n\nfsrestore <path> -D <FDS name>\n\n2. If the role of the FDS is REPLICA or the application using the FDS is capable of re-creating the FDS contents, delete all FDS files from disk by executing the following command in the same node the FDS is running:\n\n $ fshascli -l <RU>\n $ rm -f <path>/*.cp\n $ rm -f <path>/FDSlog*\n $ rm -f <path>/*.lck\n $ fshascli -u <RU>\n\nThe <RU> is the recovery unit (RU) of the FDS and it can be extracted from the MOId related to this alarm (for example, if the MOId is \n/TA-A/FSFDSTestServer/FDSTest, the <RU> is /TA-A/FSFDSTestServer). \n\nThe <path> is the path to the directory that holds the FDS files. The directory is the same as the directory of the corrupted file in the additional information field 1.		

Table 41-103 FAST_DATA_STRUCTURE_IS_CORRUPTED

Alarm	Attributes	Applicable major release
Name: FAST_DATA_STRUCTURE_IS_CORRUPTED (11682) Type: processingErrorAlarm Package: racloms.FAST_DATA_STRUCTURE_IS_CORRUPTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FAST DATA STRUCTURE IS CORRUPTED Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: FAST DATA STRUCTURE IS CORRUPTED\n\nA fast data structure (FDS) server was updating a data structure but detected that the data structure is corrupted. In most cases, this indicates that the FDS is corrupted in disk as well.\n\nThe FDS remains partially available, but all the updates and queries that concern the corrupted item will fail. The data of the FDS may also be lost.\n\nThe alarm system clears the alarm automatically when the FDS is restarted. If the next restart is not successful, the alarm will be raised again.		
Remedial action: 1. Restart the FDS\n \n $ fshascli -l <RU>\n $ fshascli -u <RU>\n\nThe <RU> is the recovery unit (RU) name of the FDS and it can be extracted from the MOId related to this alarm (for example, if the MOId is \n/TA-A/FSFDSTestServer/FDSTest, the <RU> is /TA-A/FSFDSTestServer). \n\nIf this alarm re-appears relatively soon, it might indicate that the disk copy of the FDS is corrupted. \n\n2. If the role of the FDS is MASTER or the application using the FDS is not capable of re-generating the contents of the data structure, restore the data structure from the latest backup (fsrestore <path> -D <FDS name>).\n\n3. If the role of the FDS is REPLICA or the application using the FDS is capable of re-generating the contents of the FDS, delete the corrupted FDS files by entering the following commands:\n\n $ fshascli -l <RU>\n $ rm -f <path>/*.cp\n $ rm -f <path>/FDSlog*\n $ rm -f <path>/*.lck\n $ fshascli -u <RU>\n\nThe <path> is the directory path of the FDS files.\n\n4. If the alarm still re-appears and restoring the data structure from the latest backup has already been performed, the last backup set may contain the same corruption as the original set of the FDS files. In that case, use an older backup set. \n\nIf this does not solve the problem, contact your Nokia representative.		

Table 41-104 FAST_DATA_STRUCTURE_START_UP_FAILED

Alarm	Attributes	Applicable major release
Name: FAST_DATA_STRUCTURE_START_UP_ FAILED (11683) Type: processingErrorAlarm Package: racloms.FAST_DATA_STRUCTURE_ START_UP_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FAST DATA STRUCTURE START-UP FAILED Implicitly cleared: true Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A
Description: FAST DATA STRUCTURE START-UP FAILED\n\nThe start-up of a fast data structure (FDS) server failed due to a configuration error in the start-up parameters.\n\nThe FDS does not start and client applications cannot access it.\n\nThe alarm is cleared once the fault in question has been repaired. \n\nIn this case, the application raises an alarm and then restarts, as it cannot function with the fault in question. Due to its restart, the alarm system assumes the that alarm is obsolete and clears it immediately. This process continues till the defect that caused the alarm has been removed.		
Remedial action: Contact your Nokia representative.		

Table 41-105 FIBRE_CHANNEL_CONTROLLER_ERROR

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_CONTROLLER_ERROR (11684) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_ CONTROLLER_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL CONTROLLER ERROR Implicitly cleared: false Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL CONTROLLER ERROR\n\nFibre channel (FC) controller errors exceed the threshold value. The fibre channel controller has been reset due to a severe communication deadlock.\n\nIf the problem is persistent it may affect the storage access reliability and performance.\n\nClear the alarm with the alarm management application after correcting the fault as detailed in the Instructions.		
Remedial action: Consecutive alarms indicate FC-related hardware or firmware problems. \n\nIf the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. If the alarm source is a single CPI (CPU Intel Type), check/replace it.\n2. Otherwise check/replace the Switch and Service Unit (SWSE). \nSee the corresponding adapter number in information field 1. Adapter 0 is the SWSE in slot 8 and adapter 1 is the SWSE in slot 7. \n3. Also check/replace the hard disk fibre channel (HDF) used.\n\nIf the hardware is IBM Blade Center, then follow these instructions:\n1. Check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If all cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n\nRefer to the hardware maintenance documentation for detailed replacement instructions.\n\nIf the faulty component cannot be identified and the situation is not resolved, contact your local Nokia representative.		

Table 41-106 FIBRE_CHANNEL_DEVICE_ERROR

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_DEVICE_ERROR (11685) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_DEVICE_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL DEVICE ERROR Implicitly cleared: false Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL DEVICE ERROR\n\nFibre channel (FC) device errors have exceeded the threshold value. The FC driver has detected unexpected behaviour such as direct memory access (DMA) underflow, device queue overflow, unknown command completion status, or unknown packet completion bits.\n\nIf the problem is persistent, it may affect storage access reliability and performance.\n\nClear the alarm with the alarm management application after correcting the fault as detailed in the Instructions.		
Remedial action: Consecutive alarms indicate FC related hardware or firmware problems. \n\nIf the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. If the alarm source is a single CPI (CPU Intel Type), check/replace it.\n2. Otherwise, check/replace Switch and Service Unit (SWSE). See the corresponding adapter number in information field 1. Adapter 0 is the SWSE in slot 8 and adapter 1 is the SWSE in slot 7. \n3. Also check/replace the hard disk fibre channel (HDF) used.\n\nIf the hardware is IBM Blade Center, then follow these instructions:\n1. Check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If all cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n\nRefer to the hardware maintenance documentation for detailed replacement instructions.\n\nIf the faulty component cannot be identified and the situation is not resolved, contact your local Nokia representative.		

Table 41-107 FIBRE_CHANNEL_FRAME_TRANSMISSION__CRC__ERROR

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_FRAME_TRANSMISSION__CRC__ERROR (11686) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_FRAME_TRANSMISSION__CRC__ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL FRAME TRANSMISSION (CRC) ERROR Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL FRAME TRANSMISSION (CRC) ERROR\n\nThe threshold value of the fibre channel (FC) cyclic redundancy check (CRC) error counter has been exceeded. The system has detected an excessive number of corrupted FC frames within a server node. Resetting nodes commonly causes some frames to be incomplete, resulting in CRC errors.\n\nNote that in addition to equipment failure this alarm can result from an abruptly terminated frame transmission caused by a lower level FC operation (for example, a loop initialisation).\n\nThis alarm indicates that an excessive number of CRC errors has been detected. If the problem is persistent it may affect storage access reliability and performance.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This is an informative alarm which does not require any direct actions.\nHowever, consecutive alarms might indicate FC-related hardware or firmware problems, especially if other FC related alarms are raised as well. \n \nIf the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. If the alarm source is a single CPI (CPU Intel Type), check it and replace it if necessary.\n2. Otherwise, check the Switch and Service Unit (SWSE) and replace it if necessary. See the corresponding adapter number in additional information field 1. Adapter 0 is the SWSE in slot 8 and adapter 1 is the SWSE in slot 7. \n3. Also check/replace the hard disk fibre channel (HDF) used.\n\nIf the hardware is IBM Blade Center, then follow these instructions:\n1. Check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If all cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n\nRefer to the hardware maintenance documentation for detailed replacement instructions.\n\nIf the faulty component cannot be identified and the situation is not resolved, contact your local Nokia representative.		

Table 41-108 FIBRE_CHANNEL_LINK_ERROR

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_LINK_ERROR (11687) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_LINK_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL LINK ERROR Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL LINK ERROR\n\nThe fibre channel (FC) link errors have exceeded the threshold value. The link errors result from basic signal-related problems, such as loss of signal, loss of synchronisation, and link timeout errors.\n\nThe recovery at link level disturbs the normal frame flow. If the problem is persistent, it may affect storage access reliability and performance.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This is an informative alarm and does not require direct actions. \nHowever, consecutive alarms might indicate FC-related hardware or firmware problems, especially if other FC-related alarms are raised as well. \n\nIf the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. If the alarm source is a single CPI (CPU Intel Type), check it and replace it if necessary.\n2. Otherwise, check the Switch and Service Unit (SWSE) and replace it if necessary.\nSee the corresponding adapter number in additional information field 1. Adapter 0 is the SWSE in slot 8 and adapter 1 is the SWSE in slot 7. \n3. Check the hard disk fibre channel (HDF) and replace it if necessary.\n\nIf the hardware is IBM Blade Center, then follow these instructions:\n1. Check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If all cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n \nRefer to the hardware maintenance documentation for detailed replacement instructions.\n\nIf the faulty component cannot be identified and the situation is not resolved, contact your local Nokia representative.\n\nNote that this alarm will appear if a node which has direct disk access has been bypassed in the FC loop - for example, with the swc tool of the SWSE. Follow the instructions below to check whether some nodes in a loop have been bypassed:\n\n1. Connect to the switch from /Directory:\nssh switch-0\n\n2. Check the status of the ports with the swc tool. For example:\n\n~# swc\n(RadiSys SWSE Switch) >show fibre port all\n\nFC Admin Port\nPort Mode Status\n------- ------- -------\n 1 Enable Up Inserted\n 2 Enable Up Inserted\n 3 Enable Up Inserted\n 4 Enable Up Inserted\n 5 Enable Up Inserted\n 6 Enable Up Inserted\n 9 Enable Up Inserted\n10 Disable Down Generic Bypass\n11 Enable Up Inserted\n12 Enable Up Inserted\n13 Enable Up Inserted\n14 Enable Up Inserted\n1f (Front Panel) Enable Down Manual Bypass\n2f (Front Panel) Enable Down Manual Bypass\n3f (Front Panel) Enable Down Manual Bypass\n4f (Front Panel) Enable Down Manual Bypass\nHub Interconnect Enable Up Inserted\n\n3. Exit the swc tool:\n\n(RadiSys SWSE Switch) >quit\n\n4. Execute steps 1-3 for all switches in the network element (NE).\n\nThis alarm is automatically cleared when the bypassed node is added back into the loop.		

Table 41-109 FIBRE_CHANNEL_LINK_FAILURE

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_LINK_FAILURE (11688) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_LINK_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL LINK FAILURE Implicitly cleared: true Default probable cause: LINK_FAILURE	Release: • LOMS16A
Description: FIBRE CHANNEL LINK FAILURE\n\nOne of the fibre channel switch modules has lost its connection. The error might have been caused by a hardware failure, that is, a potentially broken fibre channel switch module, a broken simple form-factor pluggable (SFP) transceiver or by an unplugged or broken fibre channel cable.\n\nUsually there are at least two fibre channel switch modules equipped and the fibre channel connection is still fully operational if at least one fibre channel link is up. However, the lost connection should be re-established as soon as possible to ensure fault tolerant operability. If the redundant connection is not re-established and the only remaining link goes down, the devices attached to the fibre channel become inaccessible.\n\nThe alarm is automatically cleared by the fault detector of the operating system when the corresponding fibre channel link comes up.		

Table 41-109 FIBRE_CHANNEL_LINK_FAILURE (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. If the alarm is raised, check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n\n2. If all the cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis\n\n4. If the previous steps have not resolved the situation, contact your local Nokia representative.		

Table 41-110 FIBRE_CHANNEL_SWITCH_PORT_STATUS_CHANGE

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_SWITCH_PORT_STATUS_CHANGE (11689) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_SWITCH_PORT_STATUS_CHANGE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL SWITCH PORT STATUS CHANGE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL SWITCH PORT STATUS CHANGE\n\nThe protocol status for some of the switch ports has changed. There can be several reasons for this alarm, such as changes in the configuration that make the port unable to process the protocol, or manually/automatically isolating the port from loop or fabric. Port Status and Port State values will give the clear reason for raising this alarm.\n\nUsually there are at least two fibre channel switch modules equipped and the fibre channel connection is still fully operational if the redundant link via the redundant switch is up. However, the redundant connection should be re-established as soon as possible to ensure fault tolerant operability. If the redundant connection is not re-established and the only remaining link goes down, the devices attached to fibre channel become inaccessible.\n\nThe alarm is automatically cleared by the system when the corresponding fibre channel port comes up. If the switch module needs to be replaced, the alarm has to be cleared manually.		
Remedial action: 1. If the value of Port Status is other than OK, the reason for triggering this alarm has to be studied properly. If the cause of the alarm appears to be in the application software or configuration, it has to be corrected.\n2. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n3. If the previous steps have not solved the situation, contact your local NSN representative.		

Table 41-111 FIBRE_CHANNEL_SWITCH_STATUS_CHANGE

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_SWITCH_STATUS_CHANGE (11690) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_SWITCH_STATUS_CHANGE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL SWITCH STATUS CHANGE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL SWITCH STATUS CHANGE\n\nThe operational status of the connectivity unit (Fibre Channel Switch) has changed. There can be several reasons for this alarm, such as changes in the configuration causing the online unit to be offline or a malfunctioning switch. Unit Status and Unit State values will give the clear reason for the alarm.\n\nUsually there are at least two fibre channel switch modules equipped in the system and the fibre channel connection is still fully operational if the redundant link via the redundant switch is up. However, the lost connection should be re-established as soon as possible to ensure fault-tolerant operability. If the redundant connection is not re-established and the only remaining link goes down, the devices attached to fibre channel become inaccessible.\n\nThe alarm is automatically cleared by the system if the fibre channel switch recovers from the malfunction. If the switch module needs to be replaced, the alarm has to be cleared manually.		

Table 41-111 FIBRE_CHANNEL_SWITCH_STATUS_CHANGE (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. If the value of Switch Status is other than OK, check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n3. If the previous steps have not solved the situation, contact your local NSN representative.		

Table 41-112 FIBRE_CHANNEL_TOTAL_LOSS_OF_SYNC

Alarm	Attributes	Applicable major release
Name: FIBRE_CHANNEL_TOTAL_LOSS_OF_SYNC (11691) Type: equipmentAlarm Package: racloms.FIBRE_CHANNEL_TOTAL_LOSS_OF_SYNC Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIBRE CHANNEL TOTAL LOSS OF SYNC Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIBRE CHANNEL TOTAL LOSS OF SYNC\n\nThe fibre channel (FC) total loss of sync has exceeded the threshold value. The synchronisation of the input signal has failed at either bit or word level.\n\nIf the problem is persistent it may affect storage access reliability and performance.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This is an informative alarm and does not require any direct actions.\nHowever, consecutive alarms might indicate FC-related hardware or firmware problems, especially if other FC-related alarms are raised as well. \n\nIf the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. If the alarm source is a single CPI (CPU Intel Type), check it and replace it if necessary.\n2. Otherwise, check the Switch and Service Unit (SWSE) and replace it if necessary. See the corresponding adapter number in the additional information field 1. Adapter 0 is the SWSE in slot 8 and adapter 1 is the SWSE in slot 7. \n3. Check the hard disk fibre channel (HDF) and replace it if necessary.\n\nIf the hardware is IBM Blade Center, then follow these instructions:\n1. Check that all fibre channel cables at the back of the chassis are properly connected to their corresponding fibre channel switch modules.\n2. If all cables are connected and the problem persists, try replacing the fibre channel SFP transceiver and the fibre channel cable.\n3. If the problem still persists, replace the affected fibre channel switch module in the chassis.\n\nRefer to the hardware maintenance documentation for detailed replacement instructions.\n\nIf the faulty component cannot be identified and the situation is not resolved, contact your local Nokia representative.		

Table 41-113 FIELD_REPLACEABLE_UNIT_UNAVAILABLE

Alarm	Attributes	Applicable major release
Name: FIELD_REPLACEABLE_UNIT_UNAVAILABLE (11692) Type: equipmentAlarm Package: racloms.FIELD_REPLACEABLE_UNIT_UNAVAILABLE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FIELD-REPLACEABLE UNIT UNAVAILABLE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: FIELD-REPLACEABLE UNIT UNAVAILABLE\n\nThe field-replaceable unit (FRU) has been removed from the system or is not healthy.\n\nFRU is a hardware component that can be removed and replaced on-site. Typical FRUs include cards, power supply units, and chassis components.\n\nSystem functionality and performance may degrade, or the system may not work at all.\n\nThe system automatically clears the alarm when the fault has been corrected.		
Remedial action: 1. Check that all the FRUs are plugged-in, and are healthy.\n\n2. If the problem exists even after following the instructions, please contact your local customer support.		

Table 41-114 FILE_SYSTEM_USAGE_OVER_LIMIT

Alarm	Attributes	Applicable major release
Name: FILE_SYSTEM_USAGE_OVER_LIMIT (11693) Type: qualityOfServiceAlarm Package: racloms.FILE_SYSTEM_USAGE_OVER_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FILE SYSTEM USAGE OVER LIMIT Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: FILE SYSTEM USAGE OVER LIMIT\n\nThe available disk space on a partition is smaller than the minimum requirement. The partition can be filled up by crashing programs, resulting to large core files, or by large log files if the rotation of logs does not function.\n\nThere is a risk that some data cannot be written on the disk.\n\nDo not clear the alarm. This alarm is automatically cleared by the operating system's fault detector once the amount of available disk space increases above the specified limit. The raising/clearing thresholds are different to prevent unnecessary trashing.		
Remedial action: 1. Run the df -h <mount point> Linux command on the node that reports the alarm to get a report of the usage of the file system disk space.\n\nSee the mountpoint in the Identifying Application Additional Information field of the alarm.\n\n2. Unnecessary files can be deleted from the mount point. \n\nTypically, there are unnecessary files in the /tmp, /var/tmp, /var/log and in /var/crash directories.\n\nNOTE: Deleting files from the mount points may damage the system that will lead to system outage. \n\nMake sure that you know and understand the file system and directory hierarchy of network elements before deleting files.\n\n3. If the alarm is not cleared, contact your Nokia representative and provide the information gathered in the previous steps.		

Table 41-115 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • LOMS16A
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 41-116 FRONTPANEL_LINK_FAULTY

Alarm	Attributes	Applicable major release
Name: FRONTPANEL_LINK_FAULTY (11694) Type: communicationsAlarm Package: racloms.FRONTPANEL_LINK_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: FRONTPANEL LINK FAULTY Implicitly cleared: true Default probable cause: LAN_ERROR	Release: • LOMS16A
Description: FRONTPANEL LINK FAULTY\n\nThe LAN (Local Area Network) monitoring software has declared a frontpanel\nlink faulty.\n\nThis is a serious condition as the redundancy level of the system is lowered due to the failed link.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-116 FRONTPANEL_LINK_FAULTY (continued)

Alarm	Attributes	Applicable major release
Remedial action: Check the severity of the alarm. \nIf the severity is WARNING, then:\nthe system is trying to recover the failed link so currently no actions are needed.\nIf the severity is MAJOR, then:\nA frontplane link consists of one of three components from which it is impossible for the system to distinguish the real cause. The components\nare:\n1. The physical frontpanel cable\n2. The physical port on the blade 1 OR a FlexiServer external peer\n3. The physical port on the blade 2 OR a FlexiServer external peer\nIf the "are_resets_enabled" parameter is true in the alarm info,\nthen the system has already tried to reset the components and the method\nof repairing the fault is to replace one or more of these components starting\nfrom the top, except if the peer is an external entity. In the case of\nan external entity, the LAN monitoring software has no influence over it.\nIf the "are_resets_enabled" is false, however, it means that no\nautomatic resets have been executed on these components and manual resets\ncould be beneficial as instructed in the hardware maintenance documentation.\n\nRefer to the hardware maintenance documentation for how to change faulty components.\nAfter replacing any components and powering on the system or restarting\na component, allow the system at least five (5) minutes to stabilise the\nfault information. During this time other alarms might appear and this\nalarm might be cancelled for a while but do not react to the other alarms.		

Table 41-117 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • LOMS16A
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 41-118 GUEST_HW_MISCONFIGURATION

Alarm	Attributes	Applicable major release
Name: GUEST_HW_MISCONFIGURATION (11697) Type: processingErrorAlarm Package: racloms.GUEST_HW_MISCONFIGURATION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: GUEST HW MISCONFIGURATION Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: GUEST HW MISCONFIGURATION\n\nVirtual OMS sets this alarm when guest machine HW configuration does not meet any of defined HW profiles (flavors).\n\n\n\n		
Remedial action: Verify the defined hardware configuration profiles (flavors) and reconfigure the OMS guest machine accordingly.		

Table 41-119 HARD_DISK_DRIVE_FAILURE

Alarm	Attributes	Applicable major release
Name: HARD_DISK_DRIVE_FAILURE (11698) Type: equipmentAlarm Package: racloms.HARD_DISK_DRIVE_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: HARD DISK DRIVE FAILURE Implicitly cleared: false Default probable cause: DISK_PROBLEM	Release: • LOMS16A
Description: HARD DISK DRIVE FAILURE\n\nThis alarm is raised when the kernel indicates that the disk has failed. The disk failure may be caused by a physically broken hard drive or a solid state disk, problem with the disk controller, device driver, or incorrect wiring. As the software cannot run with a failed hard drive, the node does not operate correctly.\n\nThe given node is not functional as the disk drive has a critical problem. The faulty node must be locked as soon as possible.\n\nClear the alarm with an alarm management application after correcting the fault as presented in the Instructions.		
Remedial action: Follow the instructions provided in customer documentation for replacing the hard drive.		

Table 41-120 ID_CONFLICT_IN_BTS_O_M_CONNECTION

Alarm	Attributes	Applicable major release
Name: ID_CONFLICT_IN_BTS_O_M_CONNECTION (11699) Type: communicationsAlarm Package: racloms.ID_CONFLICT_IN_BTS_O_M_CONNECTION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ID CONFLICT IN BTS O&M CONNECTION Implicitly cleared: false Default probable cause: COMMUNICATION_PROTOCOL_ERROR	Release: • LOMS16A
Description: ID CONFLICT IN BTS O&M CONNECTION\n\nTwo or more network elements, that try to communicate to OMS, have the same network element id.\n\nOMS can not communicate with the network elements that have the same id.\n\nClear the alarm when ID CONFLICT problem has been solved.		
Remedial action: Give unique id for the network elements.		

Table 41-121 ILLEGAL_USAGE_OF_EXTERNAL_ALARM_TIME

Alarm	Attributes	Applicable major release
Name: ILLEGAL_USAGE_OF_EXTERNAL_ALARM_TIME (11700) Type: processingErrorAlarm Package: racloms.ILLEGAL_USAGE_OF_EXTERNAL_ALARM_TIME Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ILLEGAL USAGE OF EXTERNAL ALARM TIME Implicitly cleared: false Default probable cause: SOFTWARE_PROGRAM_ERROR	Release: • LOMS16A
Description: ILLEGAL USAGE OF EXTERNAL ALARM TIME\n\nThis alarm indicates that the application has raised or cleared an alarm containing an internal MOId (Managed Object Id) and provided its own alarm time. \nIt is also raised if the application has raised or cleared an alarm originated outside of the Network Element or issued by an external alarm system, but did not provide its original alarm time.\n\nThe original alarm is discarded.\n\nClear the alarm with the alarm management application after correcting the fault as presented in Instructions.		
Remedial action: Fill in a problem report with the alarm data and send it to your Nokia representative.		

Table 41-122 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • LOMS16A
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 41-123 INCOMPLETE_OR_CORRUPTED_USER_DATA_FOR_VIRTUAL_OMS_DEPLOYMENT

Alarm	Attributes	Applicable major release
Name: INCOMPLETE_OR_CORRUPTED_USER_DATA_FOR_VIRTUAL_OMS_DEPLOYMENT (11701) Type: processingErrorAlarm Package: racloms.INCOMPLETE_OR_CORRUPTED_USER_DATA_FOR_VIRTUAL_OMS_DEPLOYMENT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INCOMPLETE OR CORRUPTED USER DATA FOR VIRTUAL OMS DEPLOYMENT Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: INCOMPLETE OR CORRUPTED USER DATA FOR VIRTUAL OMS DEPLOYMENT\n\nVirtual OMS sets this alarm when user data for virtual OMS deployment is incomplete or corrupted.\n\nVirtual OMS automatic cloud deployment was not fully successful, some adjustments\non existing system might be needed.\n\nClear the alarm with an alarm management application after correcting the fault as presented in the instructions.		
Remedial action: 1. Check the cloud-deployment output log file under /var/log/cloud-deployment.log against the deployment parameters.\n\n2a. If the OMS fails to get the deployment userdata from the metadata service, alarm is triggered by missing the following deployment parameters:\n* Cluster-id\n* OMS IP configuration (default gateway(s), IP address(es), network mask(s))\n* Public key for OMS users (Nemuadmin and _nokfsoperator)\n* Timezone\n* NTP external server IP\n* DNS external server IP\n\n2b. If the OMS was able to get deployment userdata from the metadata service, alarm is triggered because: \n* Network logic is not met for OMS IP configuration\n* Timezone is in a wrong format\n\n3. Use virtual infrastructure manager console and the root account to access virtual OMS and perform the manual post-configuration using OMS CLI scripts.\nFor details refer to the OMS Operating Documentation troubleshooting instructions.		

Table 41-124 INCORRECT_ALARM_DATA

Alarm	Attributes	Applicable major release
Name: INCORRECT_ALARM_DATA (11702) Type: processingErrorAlarm Package: racloms.INCORRECT_ALARM_DATA Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INCORRECT ALARM DATA Implicitly cleared: false Default probable cause: INVALID_PARAMETER	Release: • LOMS16A

Table 41-124 INCORRECT_ALARM_DATA (continued)

Alarm	Attributes	Applicable major release
Description: INCORRECT ALARM DATA\n\nThe alarm system has been requested to raise or clear an alarm with incorrect alarm data. One or more arguments provided with the request might have an invalid value or meaning: null or they might be empty, too long, out of specified range, contain non-printable characters, or have an incorrect format. The alarm number (Specific Problem) might also be unknown.\n\nAn incorrect format in this case means, for example, that a character value was entered where a numeric value was expected. A special case of an incorrect format is if the quotes (') surrounding the value of an info field are missing from an alarm notification record in the syslog.\n\nThe alarm which is requested to be raised or cleared with incorrect data is not processed further, but the information is put as additional info in this alarm. If the alarm number is unknown, then the actual fault for which the alarm has been raised is also left unknown.\n\nClear the alarm with the alarm management application after correcting the fault as presented in the Instructions, in other words, after sending the report to the local Nokia representative.		
Remedial action: Fill in a problem report, and then send it to your local Nokia representative.		

Table 41-125 INCORRECT_BIOS_SETTINGS

Alarm	Attributes	Applicable major release
Name: INCORRECT_BIOS_SETTINGS (11703) Type: processingErrorAlarm Package: racloms.INCORRECT_BIOS_SETTINGS Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INCORRECT BIOS SETTINGS Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: INCORRECT BIOS SETTINGS\n\nCurrent BIOS settings of underlying hardware may cause some functions to be disabled or degraded.\nThe BIOS setting enables boot from USB device with higher priority than secondary disks. This setting together with USB device inserted in USB port may break software management operation such as disk lock, cut-over, and software set activation.\n\nThe alarm is raised if FlexiPlatform verifies that BIOS was incorrectly configured, for example when USB is not disabled from boot order settings in BIOS.\n\nThe alarm is automatically canceled once the BIOS settings are found to be correct during the next checking period.		
Remedial action: Check the additional information for maintenance action details		

Table 41-126 INCORRECT_CONFIGURATION_DATA_IN_LDAP

Alarm	Attributes	Applicable major release
Name: INCORRECT_CONFIGURATION_DATA_IN_LDAP (11704) Type: processingErrorAlarm Package: racloms.INCORRECT_CONFIGURATION_DATA_IN_LDAP Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INCORRECT CONFIGURATION DATA IN LDAP Implicitly cleared: false Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A

Table 41-126 INCORRECT_CONFIGURATION_DATA_IN_LDAP (continued)

Alarm	Attributes	Applicable major release
Description: INCORRECT CONFIGURATION DATA IN LDAP\n\nThe LDAP (Lightweight Directory Access Protocol) holds incorrect configuration data for an application.\nApplications usually retrieve their configuration data from the LDAP either directly or by using configuration translation scripts that will convert the data in the LDAP into configuration files. In this case the translation script has detected that the configuration information is incorrect and the application cannot therefore function properly.\n\nThe application may be unusable or behave incorrectly due to incorrect configuration data stored in the LDAP.\nIf the error happened after issuing the fsconfigure --translate_config command the application may still be operating using the old configuration. If the old configuration was working, the application should keep running normally until restarted or switched over to another recovery unit if running in active / standby recovery group.\nIf the error happened after a cluster restart or after issuing the fsconfigure --activate_config command the application will be started using the incorrect configuration. In this case the application may fail or function incorrectly. It is recommended to lock the recovery unit / group in question to prevent damage to the system.\n\nClear the alarm with an alarm management application after correcting the fault as described in the Instructions section.		
Remedial action: If the application fails or uses the incorrect configuration lock the application recovery group with the fshascli command. For example, the /TestAppl recovery group can be locked by issuing the following command:\n$ fshascli --lock /TestAppl\nThe application configuration data in the LDAP must be corrected and the application re-activated by issuing the following fsconfigure commands:\n$ fsconfigure --translate_config\n$ fsconfigure --activate_config\nThe first command executes the configuration translation scripts that will take the corrected values into use. The second command executes activation scripts that will restart the application. Following these two commands, the corrected values should now be in use.		

Table 41-127 INSECURE_O_M_CONNECTION

Alarm	Attributes	Applicable major release
Name: INSECURE_O_M_CONNECTION (11705) Type: communicationsAlarm Package: racloms.INSECURE_O_M_CONNECTION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INSECURE O&M CONNECTION Implicitly cleared: true Default probable cause: UNSPECIFIED_REASON	Release: • LOMS16A
Description: INSECURE O&M CONNECTION\n\nNetwork element has established a connection with insecure protocol, while the mediator is configured in 'Probing' security mode. In 'Probing' mode the security connections are preferred, i.e. the alarm may be an indication of a failure in setting up a secure connection.\n\nThe O&M mediator detects an unsecure connection from a network element, while the mediator is configured in 'Probing' security mode\n\nThe alarm shall be cancelled when NE is disconnected, or the security mode is changed to 'Off' or 'Forced'		
Remedial action: The alarm may be an indication of a failure in setting up a secure connection. Check the configuration of the secure mode in the OMS and the RNC/ADA/MRBTS. The RNC/ADA/MRBTS secure mode might be in the "Off" state.		

Table 41-128 INVALID_ACTIVE_SESSIONS

Alarm	Attributes	Applicable major release
Name: INVALID_ACTIVE_SESSIONS (11706) Type: processingErrorAlarm Package: racloms.INVALID_ACTIVE_SESSIONS Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INVALID ACTIVE SESSIONS Implicitly cleared: false Default probable cause: DATABASE_ INCONSISTENCY	Release: • LOMS16A

Table 41-128 INVALID_ACTIVE_SESSIONS (continued)

Alarm	Attributes	Applicable major release
Description: INVALID ACTIVE SESSIONS\n\nCurrently there are open sessions to the network element (NE) that operates according to outdated authorisation profiles. This situation occurs when there are changes in NetAct Lightweight Directory Access Protocol (LDAP) affecting those external Remote User Information Management (RUIM) user accounts (or permissions associated with those accounts) which were replicated into the NE's local user database. The change can be one of the following:\n\nuser account has been removed in NetAct,\n\nuser account cannot be used to access the NE anymore,\n\npermissions associated with this account have changed in NetAct.\n\nCurrently there are active user sessions, opened before the above-mentioned changes were detected in the NE. Within those already created user sessions, access control changes are not automatically taken into effect. Users logged in with affected user accounts still continue to operate with the old permission set.\n\nPlease note that only sessions maintained in /var/run/utmp are monitored. Currently those are only SSH sessions (ftp sessions opened with vsftpd are also visible in /var/run/utmp, but ftp sessions are not possible with external user accounts according to the platform configuration). For other types of sessions no alarm is raised.\n\nNote: the session list in /var/run/utmp is not currently accessible with SCLI.\n\nThis alarm can indicate that some users operate within the NE with higher permissions than allowed by NetAct according to a changed user account authorisation profile. There are four possible reasons for this:\n\n1.A non-existent user is still logged into the NE (user account removed in NetAct).\n\n2.A user with no permissions for the NE is logged in (user account has been detached from the NE according to RUIM Access Control Lists).\n\n3.A user has higher permissions than defined in NetAct (permissions for the user account were lowered).\n\n4.A user has lower permissions than defined in NetAct (permissions for the user account were raised)\n\nNote that cases 1-3 indicate a security risk.\n\nAfter correcting the fault, as presented in the Instructions section, clear the alarm in NE using the following SCLI command:\n>set alarm clear alarm-id <alarm id of the alarm>\n\nIf the alarm id of the alarm is unknown, use the following SCLI command (that requires the full alarm information):\n>set alarm clear-matching-alarms filter-by specific-problem 70269 managed-object <managed object of the alarm> application-id <application id of the alarm> identifying-application-additional-info <identifying application additional info of the alarm>		
Remedial action: All currently active SSH sessions based on user accounts mentioned in the Application Additional Info field of the alarm must be closed and reopened if needed. After reopening a session correct permissions are taken into use, if the account is still in use for the NE.\n \nInitiate ssh sessions\n1.Log into the active CLA.\n2.To check the open ssh sessions, execute the following command:\n# utmpdump /var/run/utmp\nNote: there is currently no equivalent SCLI command.\n\nFor example, the result of invoking utmpdump may look as follows:\n# utmpdump /var/run/utmp\n...\n[6] [06306] [co] [LOGIN] [ttyS1] [ ] [196.144.10.0] [Tue Nov 14 16:20:58 2006 EET]\n[7] [32610] [ts/0] [testuser] [pts/0] [fle4gr01.ntc.nsn.com] [172.21.216.104] [Tue Nov 21 19:06:11 2006 EET]\n[7] [32679] [ts/1] [testuser] [pts/1] [fle4gr01.ntc.nsn.com] [172.21.216.104] [Tue Nov 21 19:07:07 2006 EET]\n[7] [32743] [ts/2] [testuser] [pts/2] [fle4gr01.ntc.nsn.com] [172.21.216.104] [Tue Nov 21 19:07:45 2006 EET]\n[7] [00361] [ts/3] [testuser] [pts/3] [fle4gr01.ntc.nsn.com] [172.21.216.104] [Tue Nov 21 19:08:50 2006 EET]\n[7] [17382] [ts/4] [root] [pts/4] [flegrp13.ntc.nsn.com] [172.21.220.61] [Fri Dec 01 14:59:47 2006 EET]\n[7] [01256] [ts/5] [extuser] [pts/5] [esfleg03.ntc.nsn.com] [172.21.216.127] [Sun Dec 03 13:05:44 2006 EET]\n[7] [04574] [ts/6] [root] [pts/6] [esfleg02.ntc.nsn.com] [172.21.216.126] [Fri Dec 01 12:29:21 2006 EET]\n\n...\n3.Preferred way of closing a session is a graceful exit. It is, however, possible to close it forcefully. The following example illustrates forceful cleanup of a session for user "extuser".\n\n4.First, check the sshd process id of the child process of "01256": \n# ps -ef | grep 1256\nroot 1256 7701 0 13:05 ? 00:00:00 sshd: extuser [priv]\n10009 1276 1256 0 13:05 ? 00:00:00 sshd: extuser@pts/5\nroot 2504 17382 0 13:06 pts/4 00:00:00 grep 1256\n\nand terminate it:\n# kill -9 1276\n\nNote: there are currently no equivalent SCLI commands.\n\nssh session for user "extuser" is terminated.		

Table 41-129 INVALID_IP_CONFIGURATION

Alarm	Attributes	Applicable major release
Name: INVALID_IP_CONFIGURATION (11707) Type: processingErrorAlarm Package: racloms.INVALID_IP_CONFIGURATION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INVALID IP CONFIGURATION Implicitly cleared: false Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A

Table 41-129 INVALID_IP_CONFIGURATION (continued)

Alarm	Attributes	Applicable major release
Description: INVALID IP CONFIGURATION\n\nThe system contains a daemon process that is responsible for creating the Internet Protocol (IP) related configuration - e.g. interfaces, addresses and routes - based on the data stored in the system lightweight directory access protocol (LDAP) directories. Note that typically all or most of this configuration data is created during the system commissioning. \nThe daemon reads the LDAP directories and creates the configuration typically during the start up phase of the system, e.g. after the system reboot. However, the configuration may also be deliberately changed in a live network element as part of maintenance operations, for example, during an upgrade of the system. \nThe daemon creating the configuration raises this alarm if it reads semantically illegal IP configuration data from the LDAP directories and cannot create such a configuration. Examples of this kind of data would be a non-existing interface or a route to such an interface.\n\nThe daemon process will ignore the illegal data and attempts to continue the configuration using other valid data. The effect and severity of the encountered error condition depends on the actual unsuccessful configuration action. \nMost likely these kinds of errors would be experienced when configuring the external connectivity (that is, external interfaces, addresses and routes) of the network element. Especially in these situations the network element would lack the required site connectivity and would not be able to fully provide the intended services.\n\nClear the alarm with an alarm management application after correcting the fault as presented in the instructions.		
Remedial action: As already indicated above, the number of potential errors in the configuration data is large. First, check carefully the additional info fields of the alarm; the daemon attempts to pinpoint the error it encountered.\nTry to identify whether the illegal data relates to the external connectivity configuration or some other "internal" configuration. The latter case is more difficult in the sense that it most likely requires re-commissioning of the entire system. Note that this situation would most likely occur during the first commissioning of the system; if this error would be encountered spontaneously e.g. after rebooting of an earlier commissioned network element, this would most likely indicate a corrupted LDAP directory. \nThe distinguished name in the alarm identifies the invalid object in LDAP which caused the alarm. Try to fix the object (or delete it if fixing seems impossible) with fsip* tools. Once the problem is fixed inform NetworkManager to reload the configuration:\n$ fsnetworkmanagerreload		

Table 41-130 INVALID_SNMP_TRAP_COMMUNITY_STRING

Alarm	Attributes	Applicable major release
Name: INVALID_SNMP_TRAP_COMMUNITY_ STRING (11708) Type: processingErrorAlarm Package: racloms.INVALID_SNMP_TRAP_ COMMUNITY_STRING Raised on class: racloms.OMS	Severity: indeterminate Specific problem: INVALID SNMP TRAP COMMUNITY STRING Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: INVALID SNMP TRAP COMMUNITY STRING\n\nThe simple network management protocol (SNMP) Mediator has received an SNMP trap that contains an invalid trap community string that does not match the community string in the SNMP Mediator's configuration. Community strings are passwords that are used to authenticate the senders of SNMP traps.\n\nIf such an invalid trap is received, it is ignored.\n\nClear the alarm with the alarm management application after correcting the fault as presented in the Instructions.		
Remedial action: 1. Check the IP address of the SNMP agent that sent the trap. The IP address is displayed in the Identifying Application Additional Information field 1 of the alarm.\n\n2. Check the community string that was received in the trap. The community string is displayed in the Application Additional Information field 2 of the alarm.\n\n3. Use the parameter management application to check the community string that the SNMP Mediator expects. Attribute fssnmpCommunityString of the\nfollowing entry defines the community string:\nfssnmpTrapSource="<agent ip / hostname>\nfssnmpAttributeType=Commstrings,\nfssnmpMediatorName=1,\ nfsFragmentId=SNMP,\nfsClusterId=ClusterRoot\n\n4. Modify the community string in the Configuration Directory to match the community string received in the trap, or configure the SNMP agent to use the community string that the SNMP Mediator expects. \n\nNote that if no community string has been specified for an IP address in the Configuration Directory, the SNMP Mediator accepts all community strings from that address."		

Table 41-131 IN_MEMORY_DATABASE_DISK_PARTITION_PROBLEM_DETECTED

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_DISK_PARTITION_PROBLEM_DETECTED (11709) Type: processingErrorAlarm Package: racloms.IN_MEMORY_DATABASE_DISK_PARTITION_PROBLEM_DETECTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE DISK PARTITION PROBLEM DETECTED Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_UNAVAILABLE	Release: • LOMS16A
Description: IN-MEMORY DATABASE DISK PARTITION PROBLEM DETECTED\n\nIn-memory database disk partition is mounted read-only or the mount point is missing.\n\nIn-memory database is not able to write to disk, checkpointing and transaction logging fail.\n\nThe system clears the alarm automatically when InMemoryDB restarts or if the problem clears itself.		
Remedial action: If the disk partition is mounted read-only, database high availability (HA) service for the in-memory database tries to correct the situation by restarting the InMemory recovery unit. If the mount point is missing, InMemoryDB RU restart may be tried to see if it clears the situation. If InMemoryDB restart does not help and the alarm is raised again contact your local NSN representative and provide them with the information you obtained alarm notification's fields.		

Table 41-132 IN_MEMORY_DATABASE_IS_ERRONEOUSLY_CONFIGURED

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_IS_ERRONEOUSLY_CONFIGURED (11710) Type: processingErrorAlarm Package: racloms.IN_MEMORY_DATABASE_IS_ERRONEOUSLY_CONFIGURED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE IS ERRONEOUSLY CONFIGURED Implicitly cleared: false Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: IN-MEMORY DATABASE IS ERRONEOUSLY CONFIGURED\n\nConfiguration of an in-memory database is missing or invalid.\n\nNone of the in-memory databases of the node containing an instance of the erroneously configured database are available.\n\nClear the alarm with alarm management application after correcting the fault as explained in the instructions.		
Remedial action: Attempt to restore the LDAP directory to the state where this problem did not exist. If the database configuration has recently been modified via the parameter management tool, undo the changes by using the parameter management tool or by restoring the LDAP Directory contents from a backup set. If the restoration did not help or cannot be done, contact your local NSN representative and provide the information you obtained from the alarm notification fields.		

Table 41-133 IN_MEMORY_DATABASE_IS_FAULTY

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_IS_FAULTY (11711) Type: processingErrorAlarm Package: racloms.IN_MEMORY_DATABASE_IS_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE IS FAULTY Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A

Table 41-133 IN_MEMORY_DATABASE_IS_FAULTY (continued)

Alarm	Attributes	Applicable major release
Description: IN-MEMORY DATABASE IS FAULTY\n\nThe watchdog process of the in-memory database cannot perform certain operation for a database. From the watchdog process point of view the database is faulty.\n\nThe database at issue is most likely unavailable for applications. In the case of a replicated database, the replication is also most likely out of service and alarm 70205 is raised for this reason. If the database role is Active, the watchdog process attempts to force a switchover of configured application recovery groups by failing the recovery units running in the same node as the faulty database instance.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This alarm is relatively general. The system logs (/var/log/master-syslog on the active CLA node) must be investigated for further details. Investigate the string "Data Manager" for error messages of the database server, and the string "TimesTenWD" for error messages of the watchdog process. The watchdog error messages are especially interesting because it contains the database ODBC-driver error messages. A typical error message is as follows:\nJun 19 08:55:57 info TA-A FSInMemoryDBaServer/TimesTenWD[16672]: DB_TestTT3 connect 1 S1000 9994 {[TimesTen][TimesTen 6.0.4 ODBC Driver][TimesTen]TT9994: Loading data store from disk into RAM in progress -- file \"db.c\", lineno 8806, procedure \"sbDbConnect()\"}, pgrp="16629, tid=1084229984, uid=0, gid=0 SQLThread.cpp:2395 DBSlave\nUse the native error code (9994 in the example above) to search for additional information from documentation of the in-memory database. The error messages should be read in conjunction with the reason code: \nDBConnectFailed: The watchdog process is not able to connect to the database. The system log should contain an error ODBC-driver error message that explains the reason for the problem.\nStartMonitoringFailed: The watchdog process is not able to execute certain SQL statements in the database. The system log should contain an error ODBC-driver error message that explains the reason for the problem.\nDBReconnectFailed: The watchdog process is not able to re-connect to the database after a failed heartbeat check. The system log should contain an error ODBC-driver error message that explains the reason for the problem.\nHeartbeatFailed: The watchdog process is not able to execute a heartbeat check for the database. The system log should contain an error ODBC-driver error message that explains the reason for the problem.\nDBSlave: The heartbeat check or SQL statement execution has timed out. The system log may contain some additional information about the watchdog process. This reason is usually not so serious as others.\nIf this alarm stays in the active alarm list and no obvious corrective actions can be derived from the system log error messages and in-memory database documentation, contact your local NSN representative and provide the information you obtained from the alarm notification fields and system log."		

Table 41-134 IN_MEMORY_DATABASE_PARTITION_GETTING_FULL

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_PARTITION_ GETTING_FULL (11712) Type: qualityOfServiceAlarm Package: racloms.IN_MEMORY_DATABASE_ PARTITION_GETTING_FULL Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE PARTITION GETTING FULL Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: IN-MEMORY DATABASE PARTITION GETTING FULL\n\nThe datastore's fill ratio has exceeded the user defined threshold. If the memory space is completely filled up before any corrective action has been done, applications using main memory database management system will notice the degradation in the level of service provided by the database management system. In the worst case, updates and inserts will be aborted and if the database management system's internal work area (referred as temporary memory partition) is exhausted, also the queries to the datastore will fail.\n\nThe alarm implies that the datastore has grown too large to fit in the memory space that has been allocated for it. If the space is completely filled up, the service level of the main memory database management system will be degraded during the time when the fault is effective.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Contact immediately your local Nokia representative and provide them with the information from the fields of this alarm notification.		

Table 41-135 IN_MEMORY_DATABASE_SERVER_IS_FAULTY

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_SERVER_IS_FAULTY (11713) Type: processingErrorAlarm Package: racloms.IN_MEMORY_DATABASE_SERVER_IS_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE SERVER IS FAULTY Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: IN-MEMORY DATABASE SERVER IS FAULTY\n\nThe in-memory database server cannot be started (reason 'UnableToStart') or died unexpectedly (reason 'UnexpectedDeath').\n\nNone of the in-memory databases of the node running the failed server are available.\n\nThe system clears the alarm automatically when the fault has been corrected. When the in-memory database watchdog process also fails this alarm is cleared, but the alarm 70159 with the explanation 'in-memory database server is faulty' is raised instead. The in-memory database watchdog tries a couple of times to start the server again couple of times before it, too, fails.		
Remedial action: Check the system logs (/var/log/master-syslog on the active CLA node) for the errors issued by the database server (search for "Data Manager") and in-memory database watchdog (search for the managed object name or string "TimesTenWD"). You can alternatively or in addition look at events that occurred before this alarm was raised. Contact your local NSN representative and provide the information you obtained from the alarm notification fields and system logs.		

Table 41-136 IN_MEMORY_DATABASE_SWITCHED_TO_LESS_RELIABLE_REPLICATION_PROTOCO

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_SWITCHED_TO_LESS_RELIABLE_REPLICATION_PROTOCO (11714) Type: qualityOfServiceAlarm Package: racloms.IN_MEMORY_DATABASE_SWITCHED_TO_LESS_RELIABLE_REPLICATION_PROTOCO Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE SWITCHED TO LESS RELIABLE REPLICATION PROTOCO Implicitly cleared: true Default probable cause: RESPONSE_TIME_EXCESSIVE	Release: • LOMS16A
Description: IN-MEMORY DATABASE SWITCHED TO LESS RELIABLE REPLICATION PROTOCO\n\nThe replication agent of a TimesTen database turned off the return service of the replication protocol used. The agent does this if the replication is stopped or a peer (replica) database does not acknowledge transactions within certain period of time. The root cause of the latter problem can be an overload situation or some other replication-related fault (alarm 70205 is raised for that). TimesTen replication is used to maintain a copy of the database for cold or hot active-standby redundancy.\n\nThe database can be used as normally but the replication protocol is less reliable and somewhat slower than normal. The slowness is caused by the fact that the database needs to write all updates to disc before it can take advantage of them. Normally it is enough to transmit the updates to the peer database; this is usually more efficient than writing to a disc. This alarm needs no immediate actions.\n\nThe system clears the alarm automatically when the return service is turned on again.		
Remedial action: Check first if alarm 70205 is raised for the same database and if it is, follow the instructions of that alarm. Otherwise, try to ascertain whether this alarm stays continuously raised or is raised and cancelled often. This alarm may be sign of performance problems in the node where the database is running, the node where the peer database is running or the local area network. Also, the timeouts related to the replication protocol may be too tight for the average workload. You may need to resolve the performance or replication protocol configuration problems by co-operating with your local NSN Customer Service Center.		

Table 41-137 IN_MEMORY_DATABASE_WATCHDOG_START_UP_FAILED

Alarm	Attributes	Applicable major release
Name: IN_MEMORY_DATABASE_WATCHDOG_START_UP_FAILED (11715) Type: processingErrorAlarm Package: racloms.IN_MEMORY_DATABASE_WATCHDOG_START_UP_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IN-MEMORY DATABASE WATCHDOG START-UP FAILED Implicitly cleared: false Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: IN-MEMORY DATABASE WATCHDOG START-UP FAILED\n\nThe in-memory database watchdog cannot start up because its start arguments are invalid.\n\nAll in-memory databases of the node of the failed watchdog process are unavailable.\n\nClear the alarm with alarm management application after correcting the fault as explained in INSTRUCTIONS.		
Remedial action: Contact your local Nokia representative and provide them with the information you obtained from the alarm notification fields.		

Table 41-138 IPMI_INTERNAL_FAILURE

Alarm	Attributes	Applicable major release
Name: IPMI_INTERNAL_FAILURE (11716) Type: equipmentAlarm Package: racloms.IPMI_INTERNAL_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: IPMI INTERNAL FAILURE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: IPMI INTERNAL FAILURE\n\nIPMI (Intelligent Platform Management Interface) internal failure has occurred.\n\nThe service level of the IPMI may have degraded. As a result, the hardware management monitoring and controlling functions may fail for the faulty plug-in unit in question.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. If the alarm is not cancelled automatically, replace the faulty plug-in unit if it can be identified. \n\nRefer to the hardware maintenance documentation for detailed replacing\ninstructions.\n\n2. If the faulty plug-in unit cannot be identified, contact your local Nokia representative.\n\nThe details of the faulty plug-in unit are found in the application additional info fields 5 to 7 of the alarm (cabinet, chassis and slot).		

Table 41-139 JUNIPER_NEW_MASTER_IN_VIRTUAL_ROUTER_REDUNDANCY_PROTOCOL_MODE

Alarm	Attributes	Applicable major release
Name: JUNIPER_NEW_MASTER_IN_VIRTUAL_ROUTER_REDUNDANCY_PROTOCOL_MODE (11717) Type: communicationsAlarm Package: racloms.JUNIPER_NEW_MASTER_IN_VIRTUAL_ROUTER_REDUNDANCY_PROTOCOL_MODE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: JUNIPER NEW MASTER IN VIRTUAL ROUTER REDUNDANCY PROTOCOL MODE Implicitly cleared: true Default probable cause: LOCAL_ALARM_INDICATION	Release: • LOMS16A

Table 41-139 JUNIPER_NEW_MASTER_IN_VIRTUAL_ROUTER_REDUNDANCY_PROTOCOL_MODE (continued)

Alarm	Attributes	Applicable major release
Description: JUNIPER NEW MASTER IN VIRTUAL ROUTER REDUNDANCY PROTOCOL MODE\n\nThere is a new switch which has taken up the role of the master in Virtual Router Redundancy Protocol (VRRP) configuration mode.\n\nThe new Master alarm indicates that the router has transitioned to 'Master' state. \nAn Owner router is assigned to forward traffic designated for the Virtual Router (VR). If the Owner is forwarding traffic for the VR, it is the Master router for that VR.\n\nOne or more prioritized Backup routers (If a Backup router is forwarding traffic for the VR), has replaced the Owner as the Master router for that VR.\n\nThe system clears the alarm automatically after its time to live has expired.		
Remedial action: This is an informative alarm. The Master IP address is the primary IP address of the Master router. This is the IP address listed as the source in VRRP advertisement, last received by this virtual router. This can be used by Network Management System (NMS) as an indication to sync with the new Master and show the switchover/failover to the user. This is just an informative alarm for the operator about this event.		

Table 41-140 JUNIPER_SWITCH_FAN_FAILURE

Alarm	Attributes	Applicable major release
Name: JUNIPER_SWITCH_FAN_FAILURE (11718) Type: environmentalAlarm Package: racloms.JUNIPER_SWITCH_FAN_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: JUNIPER SWITCH FAN FAILURE Implicitly cleared: true Default probable cause: COOLING_FAN_FAILURE	Release: • LOMS16A
Description: JUNIPER SWITCH FAN FAILURE\n\nFan failure has occurred and fan is not functional.\n\nWhen only one fan has failed, there is no service impact. The remaining fans increase speed to compensate. However, you must resolve the problem before another fan fails. This alarm is repeated every hour until the fan failure is fixed.\n\nThe system clears the alarm automatically once the fault has been corrected.		
Remedial action: To determine the source of the failure, you must physically inspect the switch, and the fuses. For more information, see the hardware installation guide for Juniper switch model at the following link:\n\nhttp://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/hardware/ex3200-ex4200.html		

Table 41-141 JUNIPER_SWITCH_FIELD_REPLACEABLE_UNIT_FAILURE_

Alarm	Attributes	Applicable major release
Name: JUNIPER_SWITCH_FIELD_REPLACEABLE_ UNIT_FAILURE_ (11719) Type: equipmentAlarm Package: racloms.JUNIPER_SWITCH_FIELD_ REPLACEABLE_UNIT_FAILURE_ Raised on class: racloms.OMS	Severity: indeterminate Specific problem: JUNIPER SWITCH FIELD REPLACEABLE UNIT FAILURE. Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: JUNIPER SWITCH FIELD REPLACEABLE UNIT FAILURE.\n\nA Field Replaceable Unit (FRU) has failed in the chassis.\n\nFRU is not powering up or is unable to load kernel.\n\nThe system clears the alarm automatically once the fault has been corrected.		
Remedial action: FRU replacement may be required.		

Table 41-142 JUNIPER_SWITCH_OVER_TEMPERATURE

Alarm	Attributes	Applicable major release
Name: JUNIPER_SWITCH_OVER_TEMPERATURE (11720) Type: environmentalAlarm Package: racloms.JUNIPER_SWITCH_OVER_ TEMPERATURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: JUNIPER SWITCH OVER TEMPERATURE Implicitly cleared: true Default probable cause: HIGH_TEMPERATURE	Release: • LOMS16A
Description: JUNIPER SWITCH OVER TEMPERATURE\n\nThe temperature of the switch has risen beyond acceptable conditions.\n\nThe service impact of this alarm depends on the temperature of the switch. In general, the switch increases the speed of the fans when any component exceeds 55 °C. The fans remain at a higher speed until the temperature decreases below the threshold. In this case, there is no service impact. However, if the temperature exceeds 75 °C, the switch transmits a warning and automatically shuts down. This scenario creates a significant service impact because the shutdown affects additional switches and equipment. This alarm is repeated every minute until the temperature is brought down to normal.\n\nThe system clears the alarm automatically once the fault has been corrected.		
Remedial action: To determine the source of the high temperature, you must physically inspect the switch to check if any fan has failed in the switch.		

Table 41-143 JUNIPER_SWITCH_POWER_SUPPLY_FAILURE_

Alarm	Attributes	Applicable major release
Name: JUNIPER_SWITCH_POWER_SUPPLY_ FAILURE_ (11721) Type: equipmentAlarm Package: racloms.JUNIPER_SWITCH_POWER_ SUPPLY_FAILURE_ Raised on class: racloms.OMS	Severity: indeterminate Specific problem: JUNIPER SWITCH POWER SUPPLY FAILURE. Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: JUNIPER SWITCH POWER SUPPLY FAILURE.\n\nPower supply failure can occur from one of the following:\n\n- switch circuit breaker failure\n- power circuit failure\n- power outage\n\nWhen only one of the power supplies has failed, the service impact is minimal. One power supply can provide the necessary power for a fully loaded switch. To determine the source of the failure, you must physically inspect the switch. This alarm is repeated every hour until the power supply is restored.\n\nThe system clears the alarm automatically once the fault has been corrected.		
Remedial action: To determine the source of the failure, you must physically inspect the switch, taking care to check the fuses. See the hardware installation guide for Juniper switch model for more information.		

Table 41-144 LDAP_DATABASE_CORRUPTED

Alarm	Attributes	Applicable major release
Name: LDAP_DATABASE_CORRUPTED (11722) Type: processingErrorAlarm Package: racloms.LDAP_DATABASE_CORRUPTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: LDAP DATABASE CORRUPTED Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A

Table 41-144 LDAP_DATABASE_CORRUPTED (continued)

Alarm	Attributes	Applicable major release
Description: LDAP DATABASE CORRUPTED\n\nA primary or secondary LDAP (Lightweight Database Access Protocol) database is corrupted and cannot be accessed anymore. An LDAP database can get corrupted, for example, when: \n- a disk becomes full while the database is being updated\n- a node failure and/or ungraceful node restart happens while the database is being updated\n\nThe identified LDAP database is currently unavailable. \nIn case of a secondary database, the only impact is that the node start-ups can take slightly longer because some platform services attempt to use the secondary database(s) by default.\nFailure of the primary database has a more significant impact. Most application processes cannot be (re)started anymore and applications that update LDAP will fail. If a secondary database is still available, nodes can still be (re)started but only basic platform services will be able to start.\nIf the primary and all secondary databases have failed, the network element (the cluster or any of the nodes) cannot (re)start anymore. \nThe system will next automatically try to recover the corrupted database from an operational primary or secondary database.\n\nThe alarm is cleared automatically if the automatic recovery operation is successful. The alarm must be cleared manually, in case the database has to be manually restored from a backup.		
Remedial action: The system will automatically attempt to recover the corrupted database from a functional copy. If the automatic recovery is successful, this alarm is automatically cleared and the system raises a new "CORRUPTED LDAP DATABASE RECOVERED" warning alarm. The automatic recovery, if successful, takes less than a minute. \nIf the primary and secondary database(s) are all corrupted you, must restore them from a backup. DO NOT ATTEMPT TO RESTART THE CLUSTER OR ANY OF ITS NODES BEFORE ENSURING THAT THE PRIMARY DATABASE IS OPERATIONAL. The applications can still be providing service normally and a service interruption only happens if an unsuccessful restart attempt is made.\nNotice, however, that the automatic recovery will fail if the node or database disk has become full. In this case, you can attempt to solve the situation by making space to the disk, and then allowing the system to retry automatic recovery. To do this, perform the following steps:\n1. Log into the node that has the corrupted database as root user. For example, log into the node (usually CLA-0 or CLA-1) where the directory service is active:\nssh root@mycluster-directory\n<password>\n2. Check the available disk space with the "df" command, for example:\ndf -k\nroot@CLA-1(mycluster):~# df -k \nFilesystem 1k-blocks Used Available Use% Mounted on\n/dev/rd/0 15863 10698 4346 72% /\ntmpfs 1029260 8 1029252 1% /tmp\n/dev/md/0 4999712 1401348 3598364 29% /var/mnt/local/localimg\ndirectory:/var/mnt/local/sysimg\n 49998408 49998408 0 100% /var/mnt/remote/sysimg_rw\ndirectory:/var/mnt/local/sysimg\n 49998408 49998408 0 100% /var/mnt/remote/sysimg_ro\n/dev/md/1 49998404 49998408 0 100% /var/mnt/local/sysimg\n/dev/md/9 19999256 32840 19966416 1% /var/mnt/local/backup\n3. If the database partition (in this example the system image partition) is full, release space, for example, by deleting excess core and syslog files. You can locate large files from the partition using the "find" command: Use the "cd" command to go to the partition mount point directory and search files below it, for example,\ncd /var/mnt/local/sysimg\nfind . -type f -name "syslog*" -size +1000000\nYou can also locate core files using the "find" command, for example,\ncd /var/mnt/local/sysimg\nfind . -type f -name "*core"\nWhen the disk has at least 100 MB of free space, make the system trying the recovery: \n- In case of a secondary database, reboot the node. For example, execute the following command:\nshutdown -r now \n- In case of the primary database, use fshascli command to restart the Directory service: \nfshascli -rnF /Directory \nNote that this will terminate your terminal connection, thus you will need to log in again.\nIf the database was not corrupted because of a full disk, or the automatic recovery fails again, for example, because all LDAP databases are corrupted, you must restore the databases from a backup copy. For instructions on the restore process, see the backup and restore customer documentation.		

Table 41-145 LICENCE_DATA_IS_CORRUPTED

Alarm	Attributes	Applicable major release
Name: LICENCE_DATA_IS_CORRUPTED (11723) Type: processingErrorAlarm Package: racloms.LICENCE_DATA_IS_CORRUPTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: LICENCE DATA IS CORRUPTED Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: LICENCE DATA IS CORRUPTED\n\nThe configuration of licence management contains corrupted licence data.\n\nIf corrupted licence data is detected in the configuration of licence management, the network element does not take the licence into use. \n\nAs a result, the application implementing the licensed feature may not operate properly. The feature capacity usage may also be affected.\n\nAfter correcting the fault as presented in Instructions, clear the alarm with alarm management application.		

Table 41-145 LICENCE_DATA_IS_CORRUPTED (continued)

Alarm	Attributes	Applicable major release
Remedial action: Fill in a problem report and send it to your local Nokia representative.		

Table 41-146 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • LOMS16A
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 41-147 LICENSE_MANAGEMENT_INTERNAL_MESSAGE_AUTHENTICATION_FAILED

Alarm	Attributes	Applicable major release
Name: LICENSE_MANAGEMENT_INTERNAL_ MESSAGE_AUTHENTICATION_FAILED (11724) Type: processingErrorAlarm Package: racloms.LICENSE_MANAGEMENT_ INTERNAL_MESSAGE_AUTHENTICATION_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: LICENSE MANAGEMENT INTERNAL MESSAGE AUTHENTICATION FAILED Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: LICENSE MANAGEMENT INTERNAL MESSAGE AUTHENTICATION FAILED\n\nAn attempt to tamper with the communication between the license manager server and the application implementing the licensed feature has been detected.\n\nThe application implementing the licensed feature may not operate properly.\n\nAfter correcting the fault as presented in Instructions, clear the alarm with alarm management application.		
Remedial action: Fill in a problem report and send it to your local Nokia representative.		

Table 41-148 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • LOMS16A

Table 41-148 LinkDown (equipment) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 41-149 MAJOR_SW_UPGRADE_DATA_IMPORT_FAILURE

Alarm	Attributes	Applicable major release
Name: MAJOR_SW_UPGRADE_DATA_IMPORT_ FAILURE (11725) Type: processingErrorAlarm Package: racloms.MAJOR_SW_UPGRADE_DATA_ IMPORT_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MAJOR SW UPGRADE DATA IMPORT FAILURE Implicitly cleared: false Default probable cause: INVALID_PARAMETER	Release: • LOMS16A
Description: MAJOR SW UPGRADE DATA IMPORT FAILURE\n\nImporting configuration data to LDAP database has partly failed when performing major software upgrade.\n\nThe seriousness of the alarm varies depending on the data, which importing has failed. It may vary from serious problem(s) in cluster availability to loss of configuration data of single subsystem.\n\nClear the alarm with an alarm management application after correcting the fault as presented in instructions field.		
Remedial action: 1. Log into the cluster. \nIn worst case, you might need a console connection to do this. \n2. Check from additional information field in which phase the import has failed. Usually pre-phase indicates a more serious problem.\n3. Check the fp_import and postconfig logs in /var/log directory for more detailed information.\n4. After fault analysis and corrective action(s), execute fsswcli --major --postconfigure again.		

Table 41-150 MANAGED_OBJECT_FAILED

Alarm	Attributes	Applicable major release
Name: MANAGED_OBJECT_FAILED (11726) Type: processingErrorAlarm Package: racloms.MANAGED_OBJECT_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MANAGED OBJECT FAILED Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ ABNORMALLY_TERMINATED	Release: • LOMS16A

Table 41-150 MANAGED_OBJECT_FAILED (continued)

Alarm	Attributes	Applicable major release
Description: MANAGED OBJECT FAILED\n\nThe named managed object has failed. The managed object can be a software, hardware, or logical entity. The type of managed object identifies the following: \n\nNode: The physical computing node, its system software or operating system has failed, or the node has been manually restarted. \n\nRecovery unit (RU): A recovery unit contains one or more processes. A recovery unit failure is usually caused by a process failure. \n\nProcess: The process has crashed, terminated abnormally, or stopped responding.\n\nRecovery group (RG): A recovery group consists of one or more recovery units. A recovery group failure alarm is raised for an active-standby configuration, when both redundant components (recovery units of the recovery group) have failed. This is always a serious situation, as it indicates a double failure (for example two nodes have failed at the same time).\n\nThe effect of the situation depends on the managed object type:\n\nNode: Any important services/functions that are provided with an active-standby or N+M recovery group may be taken over by other operational nodes. Services may be down if standby/spare nodes are also down. \n\nRecovery unit (RU): If the recovery unit belongs to an active-standby or N+M recovery group, the service may be taken over by an operational standby/spare recovery unit.\n\nProcess: The service or function that the process provides is not available. A process failure can cause a recovery unit level recovery action, or the system may attempt to restart the failed process.\n\nRecovery group (RG): The service provided by the recovery group is not available. Manual correction is required, as the automatic system repair actions have not solved the problem.\n\nThe system high availability services (HAS) will periodically attempt to solve the problem with corrective actions, such as switchovers or restarts. The alarm system also clears the obsolete alarms that may have been raised by this managed object, or by its child managed objects.\n\nThe system automatically clears the alarm when the fault has been corrected.		
Remedial action: 1. Log in to the cluster, and check that the named managed object has been successfully restarted. \n\n2. Verify also that the MO did not raise any new alarms that would explain the failure. You can check the status of an MO with the HAS user interface tool fshascli. An operational MO has the value ENABLED in the operational state attribute and in an empty procedural status attribute. \n\nFor example, the state of the process NodeDNS in the recovery unit FSNodeDNSServer of the node AS-5 can be seen as follows: \n$ fshascli --state /AS-5/FSNodeDNSServer/NodeDNS \n/AS-5/FSNodeDNSServer/NodeDNS:\nadministrative(UNLOCKED) \noperational(ENABLED) \nusage(ACTIVE) \nprocedural() \navailability( ) \nunknown(FALSE) \nrole(ACTIVE)\n\nIf the MO is not operational, perform the following steps:\n \n1. With a node MO, you can wait for a node restart. The system will raise another alarm (70011 NODE NOT RESPONDING) if the node does not come up within some time.\n\n2. Check the system logs (/var/log/master-syslog on the active CLA node) for error(s) that have occurred, by searching for the MO's name and/or by looking at events that occurred before this alarm was raised.\n\n3. You can also use the HAS user interface tool to initiate an immediate restart attempt of the failed MO using the -r (--restart) command line option: \n$ fshascli --restart /AS-5/FSNodeDNSServer\n\nThe restart operation is mostly useful after a problem has been corrected. Verify the result from the syslog, and by checking the status of the MO.\n\n4. Alarm for a recovery group implies a multiple error situation (for example, multiple node failures) or a persistent configuration, or corruption problem. In this case, contact your Nokia representative for assistance.		

Table 41-151 MANAGED_OBJECT_LOCKED

Alarm	Attributes	Applicable major release
Name: MANAGED_OBJECT_LOCKED (11727) Type: processingErrorAlarm Package: racloms.MANAGED_OBJECT_LOCKED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MANAGED OBJECT LOCKED Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ABNORMALLY_TERMINATED	Release: • LOMS16A
Description: MANAGED OBJECT LOCKED\n\nThe administrative state of the named managed object (MO) which can be a cluster, a node, or a recovery unit (RU) has changed to LOCKED as a result of a user action (graceful shutdown or lock operation).\n\nThe named MO and its child MOs have been stopped and will not be started before a corresponding unlock operation is performed by the user. The service provided by the MO is not available, unless the MO is a RU with some operational and UNLOCKED redundant resources. \n\nWhen an MO is locked, the alarm system of the cluster clears the alarms raised by the MO and its child MOs.\n\nDo not clear the alarm. This is an informative alarm and will be cleared automatically by the alarm system after its time to live has expired.		
Remedial action: This is an informative alarm and does not require any actions.		

Table 41-152 MANAGED_OBJECT_SHUTDOWN_BY_OPERATOR

Alarm	Attributes	Applicable major release
Name: MANAGED_OBJECT_SHUTDOWN_BY_OPERATOR (11728) Type: qualityOfServiceAlarm Package: racloms.MANAGED_OBJECT_SHUTDOWN_BY_OPERATOR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MANAGED OBJECT SHUTDOWN BY OPERATOR Implicitly cleared: true Default probable cause: CONGESTION	Release: • LOMS16A
Description: MANAGED OBJECT SHUTDOWN BY OPERATOR\n\nThis is an informative alarm which indicates that the specified managed object (MO) is being shutdown. The MO can be to the whole cluster, a node, or a recovery unit (RU). The named MO and all its unlocked sub-resources are now terminating.\n\nThe MO is being shutdown by an operator. All services provided by the named MO are terminating. Once the operation is completed, the administrative state of the MO and all its sub-MOs will be changed to locked. \n\nNote that a shutdown request may take a long time if the maximum duration for the operation has not been specified. The shutdown request can be forced to completion by issuing a lock command. In that case the platform high availability services (HAS) will terminate the services ungracefully.\n\nThe alarm system clears this alarm automatically after its time to live has expired.		
Remedial action: This is an informative alarm which requires no user actions.		

Table 41-153 MANAGED_OBJECT_UNLOCKED_BY_OPERATOR

Alarm	Attributes	Applicable major release
Name: MANAGED_OBJECT_UNLOCKED_BY_OPERATOR (11729) Type: qualityOfServiceAlarm Package: racloms.MANAGED_OBJECT_UNLOCKED_BY_OPERATOR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MANAGED OBJECT UNLOCKED BY OPERATOR Implicitly cleared: true Default probable cause: CONGESTION	Release: • LOMS16A
Description: MANAGED OBJECT UNLOCKED BY OPERATOR\n\nThis is an informative alarm which indicates that the specified managed object (MO) which can be the whole cluster, a node, or a recovery unit (RU) has been unlocked. The named MO and its unlocked sub-resources (if there are any) can now be activated.\n\nNotice that the MO (or its sub-MOs) can remain locked because of the dependency on a higher level MOs. That is, the unlock operation will not have effect on the MO in question before the higher level MOs are unlocked. For example, an RU in a node will remain locked, if the node or the cluster MO is locked.\n\nThe MO has been set to the unlocked state. If all the higher level MOs are unlocked as well, the services provided by the MO are activated.\n\nThe alarm system clears the alarm automatically after its time to live has expired.		
Remedial action: This is an informative alarm and does no require any actions.		

Table 41-154 MANUAL_NODE_ISOLATION_VERIFICATION_NEEDED

Alarm	Attributes	Applicable major release
Name: MANUAL_NODE_ISOLATION_VERIFICATION_NEEDED (11730) Type: equipmentAlarm Package: racloms.MANUAL_NODE_ISOLATION_VERIFICATION_NEEDED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MANUAL NODE ISOLATION VERIFICATION NEEDED Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A

Table 41-154 MANUAL_NODE_ISOLATION_VERIFICATION_NEEDED (continued)

Alarm	Attributes	Applicable major release
Description: MANUAL NODE ISOLATION VERIFICATION NEEDED\n\nThe platform high availability services (HAS) subsystem is unable to reset a faulty node with Intelligent Platform Management Interface (IPMI). The operational state of the node is not known, and therefore, it is not known if the node still holds and/or updates the shared resources. \n\nThis is a severe platform error that may result, for example, from:\n\n- a double hardware fault, \n- an IPMI configuration error, \n- a network partitioning problem or \n- manual power-off of a complete chassis. \n\n\nAs the HAS subsystem is not able to determine the state of the node, the active/standby recovery groups (RG) are delaying the switchovers until the node has become operational again or the node is manually set to isolation state.\n\nThe possible active/standby RGs, which have an active recovery unit (RU) instance running on the failed node, cannot recover from the situation by applying a switchover to another node. The services provided by these RGs are currently down.\n\nAlarm is cancelled automatically. \n\nIf the automatic cancellation does not succeed then after correcting the fault clear the alarm using the following SCLI command:\n\nset alarm clear alarm-id <alarm id of the alarm>\n\nIf the alarm id of the alarm is unknown, use the following SCLI command\n(that requires the full alarm information):\n\nset alarm clear-matching-alarms filter-by specific-problem <concrete\nspecific problem> managed-object\n<managed object of the alarm> application-id <application id of\nthe alarm> identifying-application-additional-info <identifying application\nadditional info of the alarm>		
Remedial action: The node may currently restart, but this cannot be verified by HAS. The immediate priority is to ensure that services can be activated. If the node becomes available, which happens if the node is merely restarting, HAS performs recovery actions, and no user action is required.\n\nHowever, if the node does not restart itself within a few minutes, HAS recovery operations will be pending, waiting for the verification that the node has been isolated (that is, it cannot access any databases or other shared resources). In this case, you must manually verify that the node is down:\n\n- press the hot swap button of the blade \n- remove the blade and wait for a while \n- re-insert the blade\n\nOnce the node has been reset, set it to the isolation state by using the command line interface:\n\n1. Log into the cluster \n\n2. Set the node to the isolated state by using the following SCLI command: \n\n> set has isolate managed-object /AS-10 \n\nAfter the node isolation has been set, HAS performs recovery actions that were pending because of this node. \n\n3. Check from the cluster syslog (/var/log/master-syslog) that no errors were reported following the node isolation. Node isolation will leave log entries, such as: \n\n INFO Managed object - set isolated - operation initiated. Target="/AS-10 \n INFO Managed object - set isolated - operation completed. Target=/AS-10 \n\nNote that if the isolation state of a node is set without actually verifying that the node is down, some serious data corruption may happen.\n \nContact your Nokia representative for finding out the reason for the failure."		

Table 41-155 MAXIMUM_THRESHOLD_HAS_BEEN_CROSSED

Alarm	Attributes	Applicable major release
Name: MAXIMUM_THRESHOLD_HAS_BEEN_ CROSSED (11731) Type: qualityOfServiceAlarm Package: racloms.MAXIMUM_THRESHOLD_HAS_ BEEN_CROSSED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MAXIMUM THRESHOLD HAS BEEN CROSSED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: MAXIMUM THRESHOLD HAS BEEN CROSSED\n\nA maximum threshold crossing, based on the threshold rule defined for the measurement result, has been detected. The seriousness of this alarm depends on the measurement(s) that reached the defined threshold value.\n\nThe precise effect of this alarm cannot be determined since the nature of the alarm depends on the measurement(s) involved in the measurement result.\n\nThe system clears the alarm automatically when the measurement result goes down and is continuously held at the maximum threshold clearing level or below.		
Remedial action: The user has configured the threshold rules so that the events the user is interested in will be notified. As a result, any detailed instructions cannot be given. \n\nUse the performance management application to get detailed information on the measurement(s) that caused this alarm.		

Table 41-156 MEASUREMENT_DATA_ERROR

Alarm	Attributes	Applicable major release
Name: MEASUREMENT_DATA_ERROR (11732) Type: processingErrorAlarm Package: racloms.MEASUREMENT_DATA_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MEASUREMENT DATA ERROR Implicitly cleared: true Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: MEASUREMENT DATA ERROR\n\nMeasurement file could not be processed.\n\nSome measurement data could have been lost due to invalid measurement file content.\n\n-		
Remedial action: Do not clear the alarm. Alarm System will clear the alarm automatically.		

Table 41-157 MEASUREMENT_DATA_NOT_TRANSFERRED

Alarm	Attributes	Applicable major release
Name: MEASUREMENT_DATA_NOT_ TRANSFERRED (11733) Type: qualityOfServiceAlarm Package: racloms.MEASUREMENT_DATA_NOT_ TRANSFERRED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MEASUREMENT DATA NOT TRANSFERRED Implicitly cleared: true Default probable cause: QUEUE_SIZE_EXCEEDED	Release: • LOMS16A
Description: MEASUREMENT DATA NOT TRANSFERRED\n\nThe number of files waiting to be transferred to NetAct has exceeded a defined threshold.\n\nSome measurement data may not have been transferred to NetAct or file transfer acknowledgments from NetAct to OMS are not working correctly.\n\nDo not clear the alarm. Alarm System will clear the alarm when the amount of untransferred files decreases below a defined threshold.		
Remedial action: If NetAct connection is wanted to be disabled, the alarm will get cancelled automatically within 10 minutes after setting LDAP parameter PMFileBufferAlarmEnabled to value 0 (zero).		

Table 41-158 MEASUREMENT_THRESHOLD_MONITORING_LIMIT_EXCEEDED

Alarm	Attributes	Applicable major release
Name: MEASUREMENT_THRESHOLD_ MONITORING_LIMIT_EXCEEDED (11734) Type: qualityOfServiceAlarm Package: racloms.MEASUREMENT_THRESHOLD_ MONITORING_LIMIT_EXCEEDED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MEASUREMENT THRESHOLD MONITORING LIMIT EXCEEDED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A

Table 41-158 MEASUREMENT_THRESHOLD_MONITORING_LIMIT_EXCEEDED (continued)

Alarm	Attributes	Applicable major release
Description: MEASUREMENT THRESHOLD MONITORING LIMIT EXCEEDED\n\nWhen this alarm has been triggered, it means that a threshold monitoring rule has been evaluated as true by OMS for some WCDMA cell object in some other RNW measurement than Cell Resource measurement for which threshold limit breaks are reported with alarm WCEL THRESHOLD MONITORING LIMIT EXCEEDED. More information on the event can be seen with the NE Threshold Management application in OMS Element Manager.\n\nThreshold monitoring makes it easier to detect faults, identify bottlenecks and optimise the network. Using OMS Element Manager GUI, appropriate performance thresholds are determined for each important variable, and exceeding these thresholds indicates a problem worth of attention. These variables can be either single counters or Key Performance Indicators (KPIs), which can be a combination of several counters.\n\nWhen performance data is gathered on variables of interest from the measured objects in the network, their values are compared against any active threshold limits. When a performance threshold is exceeded, an alarm is generated and sent to the network management system. In addition to this, a threshold event log is saved in the network element for further study of the events which have occurred in that NE during a certain period of time.\n\n-\n\nDo not clear the alarm. This alarm has a lifetime of 65 minutes.		
Remedial action: Threshold alarm does not necessarily mean that there are problems in the network element, because thresholds can be freely set by the operator, and some rules may have been set incorrectly.\n\nTo get further information on the reason of the threshold alarm:\n\n- Connect to the network element with OMS Element Manager.\n\n- Open the NE Threshold Management application.\n\n- Select "Show Threshold Log" from the View menu and check the threshold log.\n\nWhen the target object and other information of the alarm have been checked from the log, you can obtain more information from the performance counters of measurements and, if necessary, take appropriate action to correct the problem. The counters can be browsed with RNW Measurement Presentation application or by using NetAct reporting tools.		

Table 41-159 MEMORY_ERROR

Alarm	Attributes	Applicable major release
Name: MEMORY_ERROR (11735) Type: equipmentAlarm Package: racloms.MEMORY_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MEMORY ERROR Implicitly cleared: false Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: MEMORY ERROR\n\nA memory error has been detected. The possible causes are:\n\nCorrectable error-correcting code(ECC) or other correctable memory error\nUncorrectable ECC or other uncorrectable memory error\nParity error\nMemory Scrub Failed (stuck bit)\nMemory Device Disabled\nCorrectable ECC or other correctable memory error logging limit reached\n\nThe unit may have erratic behavior or decreased functionality.\n\nClear the alarm with the alarm management application after correcting the fault, according to the instructions provided.		
Remedial action: 1. Check that the affected unit is healthy, and is plugged-in properly.\n\n2. Restart the unit, if necessary.\n\n3. Replace the unit, if necessary.\n\n4. If the problem exists even after following these instructions, please contact your local Nokia representative.		

Table 41-160 MEMORY_USAGE_OVER_LIMIT

Alarm	Attributes	Applicable major release
Name: MEMORY_USAGE_OVER_LIMIT (11736) Type: qualityOfServiceAlarm Package: racloms.MEMORY_USAGE_OVER_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MEMORY USAGE OVER LIMIT Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A

Table 41-160 MEMORY_USAGE_OVER_LIMIT (continued)

Alarm	Attributes	Applicable major release
Description: MEMORY USAGE OVER LIMIT\n\nMemory consumption is too high because some processes are using too much memory.\n\nThere is a risk that the node is unable to fulfill the tasks allocated to it because the processes cannot reserve enough memory for their use. As a result, the processes cannot perform the tasks allocated to them.\n\nDo not clear the alarm. The alarm is automatically cleared by the fault detector of the operating system when the memory usage is on a low enough level. The raising / clearing thresholds are different to prevent unnecessary trashing.		
Remedial action: 1. Run the\n"top" \nLinux command on the node that reports the alarm to view a snapshot of the current global memory. \n\nPress "M" to sort the processes in the node based on their memory resident size to check which processes consume the most memory.\n\n2. If the problem persists, contact your Nokia representative and provide them with the information gathered in the previous step.		

Table 41-161 MINIMUM_THRESHOLD_HAS_BEEN_REACHED

Alarm	Attributes	Applicable major release
Name: MINIMUM_THRESHOLD_HAS_BEEN_ REACHED (11737) Type: qualityOfServiceAlarm Package: racloms.MINIMUM_THRESHOLD_HAS_ BEEN_REACHED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: MINIMUM THRESHOLD HAS BEEN REACHED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: MINIMUM THRESHOLD HAS BEEN REACHED\n\nThis alarm indicates that a minimum threshold crossing, based on the threshold rule defined for the measurement result, has been detected. The seriousness of the alarm depends on the measurement(s) that reached the defined threshold value.\n\nThe precise effect of this alarm cannot be determined since the nature of this alarm depends on the measurement(s) involved in the measurement result.\n\nThe system clears the alarm automatically when the measurement result goes\nup and is continuously held at the minimum threshold clearing level or above.		
Remedial action: The user has configured the threshold rules so that the events the user is interested in will be notified. As a result, no detailed instructions\ncan be given.\n\nUse the performance management application to get detailed information on the measurement(s) that caused this alarm.		

Table 41-162 MissedStatsCollectionAtRecovery

Alarm	Attributes	Applicable major release
Name: MissedStatsCollectionAtRecovery (11738) Type: communicationsAlarm Package: racloms.MissedStatsCollectionAtRecovery Raised on class: racloms.OMS	Severity: minor Specific problem: PM Collection Issue while recovering available PM files Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LOMS16A
Description: PM Collection Issue while recovering available PM files\nThe alarm will be cleared automatically the next time where SAM is able to get the full list of files specified in a PIFileQuery.		
Remedial action: Please refer to the LTE Nokia Node Maintenance manual for remedial action information.		

Table 41-163 MissedStatsCollectionAtRequest

Alarm	Attributes	Applicable major release
Name: MissedStatsCollectionAtRequest (11739) Type: communicationsAlarm Package: racloms.MissedStatsCollectionAtRequest Raised on class: racloms.OMS	Severity: major Specific problem: PM Collection Issue while requesting available PM files Implicitly cleared: true Default probable cause: communicationsProtocolError	Release: • LOMS16A
Description: PM Collection Issue while requesting available PM files\nThe alarm will be cleared automatically at the next successful request.		
Remedial action: Please refer to the LTE Nokia Node Maintenance manual for remedial action information.		

Table 41-164 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 41-165 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • LOMS16A
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		

Table 41-165 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 41-166 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • LOMS16A
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 41-167 NE_CONNECTION_REJECTED

Alarm	Attributes	Applicable major release
Name: NE_CONNECTION_REJECTED (11740) Type: processingErrorAlarm Package: racloms.NE_CONNECTION_REJECTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NE CONNECTION REJECTED Implicitly cleared: true Default probable cause: CONFIGURATION_OR_CUSTOMIZING_ERROR	Release: • LOMS16A
Description: NE CONNECTION REJECTED\n\nOMS has rejected connection establishment from NE. Reason for rejection is either that OMS capacity has been exceeded or that NE tried to open connection to a secondary OMS.\n\nNetwork element connection was rejected.\n\nDo not clear the alarm. The system cancels the alarm automatically after\nits lifetime has elapsed.		
Remedial action: -		

Table 41-168 NE_O_M_CONNECTION_FAILURE

Alarm	Attributes	Applicable major release
Name: NE_O_M_CONNECTION_FAILURE (11741) Type: communicationsAlarm Package: racloms.NE_O_M_CONNECTION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NE O&M CONNECTION FAILURE Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: NE O&M CONNECTION FAILURE\n\nThis alarm is raised when the BTS O&M connection between the OMS and a network element fails.\n\nThe managed network element is not reachable by the centralized O&M systems like the OMS or the NetAct.\n\nDo not clear the alarm unless the conditions given in the instructions on the manual clearing are fulfilled. This alarm is cancelled automatically by the system after the fault has been corrected. Alarm with certificate validation failure is cancelled automatically by the system if OMS OM security mode has been set to value 'Off' and insecure O&M connection has been established successfully.		
Remedial action: Normally, the alarm does not need to be cleared but the system cancels the alarm automatically when the connection is working again. However, if the related network element is removed altogether from the network, it may be necessary to cancel the alarm manually using Element Manager.\n\nIn case of certificate validation failure this alarm is cancelled automatically by the system when valid certificates are installed to NE and secure O&M connection has been restored or alternatively alarm is cancelled automatically by the system if OMS OM security mode has been set to value 'Off' and insecure O&M connection has been established successfully. However, if IP address of NE is changed before successful connection attempt, it is necessary to cancel the alarm manually using Element Manager.		

Table 41-169 NE_O_M_UPDATE_CRL_MEDIATION_FAILURE

Alarm	Attributes	Applicable major release
Name: NE_O_M_UPDATE_CRL_MEDIATION_ FAILURE (11742) Type: communicationsAlarm Package: racloms.NE_O_M_UPDATE_CRL_ MEDIATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NE O&M UPDATE CRL MEDIATION FAILURE Implicitly cleared: true Default probable cause: TRANSMISSION_ERROR	Release: • LOMS16A
Description: NE O&M UPDATE CRL MEDIATION FAILURE\n\nThe request for Certificate Revocation List (CRL) update manually triggered from NetAct is not confirmed by NE.\n\nThe alarm is raised when OMS has not received response from NE for update CRL request or response informs about a failure in request delivery to NE. So most likely Certificate Revocation List (CRL) has not been updated in NE.\n\nThe system cancels the alarm when OMS receives manual request from NetAct for Certificate Revocation List (CRL) update and the request is successfully delivered to the given NE or when the alarm time to live expires.		
Remedial action: Verify the connectivity to the NE and manually request CRL update for given NE again.		

Table 41-170 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • LOMS16A

Table 41-170 NodeDatabaseFallbackDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 41-171 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • LOMS16A
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 41-172 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 41-173 NODE_FAILED

Alarm	Attributes	Applicable major release
Name: NODE_FAILED (11743) Type: communicationsAlarm Package: racloms.NODE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NODE FAILED Implicitly cleared: false Default probable cause: UNAVAILABLE	Release: • LOMS16A
Description: NODE FAILED\n\nExternal supervision indicates that a FlexiServer node has failed. The node is down due to a software or hardware failure.\nThe services of External supervision subsystem are used in extreme cases of supervision, when the sevices of the normally used High Availability Services (HAS) are not usable. External supervision observes the behaviour of entities and announces their failure through a known channel to an information consumer outside the network element itself.\nIn case of a CLM node failure HAS cannot raise alarms 70159 - MANAGED OBJECT FAILED and 70011 - NODE NOT RESPONDING. If another node failed the alarms might be raised in addition to this alarm.\n\nThe node and any service on the node is unreachable.\nIn case of a CLM node failure this will lead to cluster failure. Functionality of the Flexiserver cluster is seriously affected. Situation is critical as there is no access to any applications in Flexi cluster and signalling/traffic has been interrupted. CLM failure also prevents further alarms from appearing.\n\nClear the alarm with Alarm Browser after correcting the fault.		
Remedial action: 1. Restart the node.\n\n2. Investigate whether the hardware for the NODE chassis, NODE chassis switch or NODE blade is broken.\n\n3. Collect all relevant data from NODE's /var/crash to ensure that it will not be deleted in periodical system cleanups.\n\n4. Contact your Nokia representative.		

Table 41-174 NODE_NOT_RESPONDING

Alarm	Attributes	Applicable major release
Name: NODE_NOT_RESPONDING (11744) Type: equipmentAlarm Package: racloms.NODE_NOT_RESPONDING Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NODE NOT RESPONDING Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: NODE NOT RESPONDING\n\nA physical computing node has not restarted despite of restart attempts. The node may be broken, is unable to restart, or is stuck.\n\nAny important services/functions that are provided with an active-standby recovery group may have been taken over by other operational nodes. Services may be down if standby nodes are also down.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Perform the following steps to verify the state of the node: \n\n1. Log into the cluster as root user. \n\n2. Use the hwcli command to verify the state of the node. For example, the state of the node /CLA-1 can be checked as follows:\n$ hwcli CLA-0\nCLA-1: available (FlexiSvr CPI1 000157:0108 01.02)\n\n3. Previous hwcli output shows that CLA-0 node is physically available. The high availability services (HAS) of the system attempts, after about 30 minutes, to restart a failed node by issuing a power-off, power-on and restart sequence. If you do not want to wait for this, you can perform the power-off, power-on and restart sequence manually. \n\nFor example: \n$ hwcli --power off CLA-0\nATTAMPTING TO POWER OFF NODE: CLA-0\nARE YOU SURE YOU WANT TO PROCEED? [no/yes] yes\nPowering off CLA-0: OK\n\n$ hwcli --power on CLA-0\nPowering on CLA-0: OK\n\n$ hwcli --reset CLA-0\nATTAMPTING TO RESET NODE: CLA-0\nARE YOU SURE YOU WANT TO PROCEED? [no/yes] yes\nResetting CLA-0: OK\n\n4. If the node does not start within a few minutes or the hwcli does not show that the node is available, check if the CPU board has any error lights on. If it does, you can try to restore the node into service by removing and re-inserting the node. \n\n5. Contact your Nokia representative even if these operations bring the node up, because it is possible that the computing node needs to be replaced or it may, for example, need a BIOS upgrade.		

Table 41-175 NO_OPERATIONAL_RECOVERY_UNIT_FOR_SERVICE_INSTANCE

Alarm	Attributes	Applicable major release
Name: NO_OPERATIONAL_RECOVERY_UNIT_FOR_SERVICE_INSTANCE (11745) Type: processingErrorAlarm Package: racloms.NO_OPERATIONAL_RECOVERY_UNIT_FOR_SERVICE_INSTANCE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NO OPERATIONAL RECOVERY UNIT FOR SERVICE INSTANCE Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ABNORMALLY_TERMINATED	Release: • LOMS16A
Description: NO OPERATIONAL RECOVERY UNIT FOR SERVICE INSTANCE\n\nAn N+M recovery group does not have an unlocked operational recovery unit for the service instance. \nAn N+M recovery group has N active recovery units that provide service and M spare recovery units. All unlocked recovery units that have been assigned a service instance workload are active and providing service. The rest of the unlocked recovery units that have not been assigned a service instance workload are spare recovery units.\nAt this moment, the system cannot assign the workload of the named service instance to any recovery unit, because there are no unlocked operational recovery units without service assignments. This can happen, for example, in the following situations:\n- Multiple node reboots have been initiated.\n- Multiple node failures have happened.\n- One or more service instances have problems causing failures for the recovery units where it has been assigned. \n- All spare recovery units are locked when a recovery unit failure happens.\n\nThe workload associated with the named service instance (part of the service provided by the recovery group) is currently down.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: This problem can indicate one or both of the following: \n- A hardware-related situation that is, for example, caused by node reboots or node failures. In these cases, the alarm severity is MINOR and the problem is likely to disappear quickly. The severity of this alarm will be raised to MAJOR if the node(s) do not restart within a few minutes. \n- An application problem caused, for example, by a program error, a configuration error, or data corruption. In this case, the alarm severity is MAJOR and manual intervention may be needed. \nIf the severity of this alarm is MINOR, you may choose to wait a few minutes to see if the alarm is cancelled. In node reboot and transient failure situations, the system will cancel the alarm as soon as the node reboots have completed and the service instance(s) has been successfully reassigned and the recovery unit restarted.\nIf the severity of this alarm is MAJOR, perform the following steps:\n1. Log into the active CLA as root user. \n2. Check the system syslog (/var/log/master-syslog) for possible failure reasons and contact your Nokia representative if you need assistance.		

Table 41-176 NO_REPLY_TO_SNMP_REQUEST

Alarm	Attributes	Applicable major release
Name: NO_REPLY_TO_SNMP_REQUEST (11746) Type: processingErrorAlarm Package: racloms.NO_REPLY_TO_SNMP_REQUEST Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NO REPLY TO SNMP REQUEST Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: NO REPLY TO SNMP REQUEST\n\nSNMP Mediator has sent an SNMP request to an SNMP agent but it has not received a response. \nExample: \n1. A filter condition has been added for the authenticationFailure (.1.3.6.1.6.3.1.1.5.5) trap. Thus the following entry can be viewed by the parameter management tool\nfssnmpV2TrapId=".1.3.6.1.6.3.1.1.5.5\nfssnmpAttributeType=V2traps, \nfssnmpMediatorName=1,\nfsFragmentId=SNMP,\nfsClusterId=ClusterRoot\nThe filter condition is defined by the attribute fssnmpFilterCondition. fssnmpFilterCondition may have, for example, the value (.1.3.6.1.2.1.1.1.0=*Linux*). See RFC 2254 for more information about the filter syntax.\n2. The SNMP Mediator receives the authenticationFailure trap that does not contain the value of variable .1.3.6.1.2.1.1.1.0.\n3. The SNMP Mediator queries the value of .1.3.6.1.2.1.1.1.0 from the SNMP agent, but does not receive a response.\n\nThe SNMP is not able to handle the trap correctly, because it is not able to query or modify variables in the SNMP agent.\n\nClear the alarm with the alarm management application after correcting the fault."		

Table 41-176 NO_REPLY_TO_SNMP_REQUEST (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Check the IP address of the SNMP agent that sent the trap. The IP address is displayed in the Application Additional Information field 1 of the alarm.\n2. The net-snmp command line tools (snmpget, snmpset etc.) provided by the operating system may be used to verify the functioning of the SNMP agent.\n3. Use the parameter management tool to check the attributes defined for the SNMP agent. The attributes are located under the following entry: \nfssnmpNEId="<agent IP / hostname>,\ nfssnmpAttributeType=NEattrs,\nfssnmpMediatorName=1,\nfsFragmentId=SNMP,\nfsClusterId=ClusterRoot\n4. Verify that the optional attribute fssnmpUDPPort has the value that the SNMP agent is listening to. The default value is 161.\n5. Verify that the optional attribute fssnmpProtocolVersion is the same that the SNMP agent supports. The default value is V2c.\n6. Verify that the optional attributes fssnmpReadCommString and fssnmpWriteCommString are the ones that the SNMP agent expects."		

Table 41-177 NTP_TIME_SYNCHRONISATION_LEADING_TO_LDAP_REPLICATION_FAILURE

Alarm	Attributes	Applicable major release
Name: NTP_TIME_SYNCHRONISATION_LEADING_ TO_LDAP_REPLICATION_FAILURE (11747) Type: processingErrorAlarm Package: racloms.NTP_TIME_SYNCHRONISATION_ LEADING_TO_LDAP_REPLICATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NTP TIME SYNCHRONISATION LEADING TO LDAP REPLICATION FAILURE Implicitly cleared: true Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A
Description: NTP TIME SYNCHRONISATION LEADING TO LDAP REPLICATION FAILURE\n\nIf the time of the cluster differs from the time of the NTP server (Network Time Protocol) the time of the cluster will be synchronised with the NTP server. This causes the time of the cluster to shift either forwards or backwards and may lead to a failure in the replication of the LDAP server, which generates the alarm. \n\nFor example, if the cluster is commissioned with an NTP Server in the UK (GMT) and with a FEWS (field engineering workstation) from GMT+2, the time will be shifted 2 hours backwards when the cluster boots for the first time and synchronises its time with the NTP Server.\n\nThe replication of the LDAP server is not working. This means that the LDAP data in the primary and secondary LDAP databases are not synchronised. If a switchover in the Directory recovery group happens, changes that were made to LDAP data after the time was reset will be lost.\n\nDo not clear the alarm. It will be cleared automatically by the alarm system after its time to live has expired.		
Remedial action: 1. Log into the cluster.\n\n2. Go to the node where the Directory recovery group is running: \n$ ssh Directory\n\n3. Make a backup of the primary LDAP server to a file:\n$ fsLDAPBackupCreate -p -v > ldap.txt\n\n4. Use the backup of the Primary LDAP server to restore the secondary LDAP server in the node where the Directory is running:\n$ fsLDAPBackupRestore -s -v < ldap.txt\n\n5. If there is another CLA node (non-Directory CLA node) in the deployment, restore the secondary LDAP server in that node with the backup of the Primary LDAP server.\nFor example:\n$ fsLDAPBackupRestore -s -n CLA-1 -v < ldap.txt		

Table 41-178 NUMBER_OF_SYNHCRONOUS_REPLICAS_TOO_LOW

Alarm	Attributes	Applicable major release
Name: NUMBER_OF_SYNHCRONOUS_REPLICAS_ TOO_LOW (11748) Type: communicationsAlarm Package: racloms.NUMBER_OF_SYNHCRONOUS_ REPLICAS_TOO_LOW Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NUMBER OF SYNHCRONOUS REPLICAS TOO LOW Implicitly cleared: true Default probable cause: UNAVAILABLE	Release: • LOMS16A

Table 41-178 NUMBER_OF_SYNHCRONOUS_REPLICAS_TOO_LOW (continued)

Alarm	Attributes	Applicable major release
Description: NUMBER OF SYNHCRONOUS REPLICAS TOO LOW\n\nMaster fast data structure (FDS) server has lost connection to one of the Synchronous Replica FDS servers and the number of current connected Synchronous Replica is too low.\n\nClient updates to the fast data structure cannot be made.\n\nWhen the number of connected Synchronous replicas is in the level of the required number, the alarm will be cleared.		
Remedial action: 1. Check that the node where the replica in question should be running has started properly and that the connection between the nodes is working. \n2. If that does not help, contact your local Nokia representative and provide them with the information from the alarm notification's fields.		

Table 41-179 NWI3_NOTIFICATION_MISSING

Alarm	Attributes	Applicable major release
Name: NWI3_NOTIFICATION_MISSING (11749) Type: communicationsAlarm Package: racloms.NWI3_NOTIFICATION_MISSING Raised on class: racloms.OMS	Severity: indeterminate Specific problem: NWI3 NOTIFICATION MISSING Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: NWI3 NOTIFICATION MISSING\n\nThe OMS sends notifications to the NMS when the configuration in the network element has been updated. The notification event is related to either configuration or topology changes in the network element. The alarm is set if all the notifications related to the configuration and topology changes cannot be sent to the NMS. The reason is notification handling error in the OMS or in the NMS. The alarm is set for OMS.\n\nThere might be incoherent information in the NMS about the network configuration and/or topology.\n\nThe alarm does not need to be cleared, but the system cancels the alarm automatically when the error situation is cleared.		
Remedial action: Upload the information related to the NWI3 fragment in question from the NMS to get the configuration information from network elements up-to-date.		

Table 41-180 OMS_ALARM_UPLOAD_FROM_NE_FAILED

Alarm	Attributes	Applicable major release
Name: OMS_ALARM_UPLOAD_FROM_NE_FAILED (11750) Type: communicationsAlarm Package: racloms.OMS_ALARM_UPLOAD_FROM_ NE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: OMS ALARM UPLOAD FROM NE FAILED Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: OMS ALARM UPLOAD FROM NE FAILED\n\nAlarm upload from NE to OMS has failed.\n\nActive alarm situation between NE and OMS may be out of synchronization.\n\nManual clearing is not necessary. Alarm is cleared automatically when next time alarm upload from NE to OMS succeeds or when Time-to-Live has passed.		
Remedial action: Check the cause of failure from Application Additional Information field.		

Table 41-181 OMS_FILE_TRANSFER_CONNECTION_COULD_NOT_BE_OPENED

Alarm	Attributes	Applicable major release
Name: OMS_FILE_TRANSFER_CONNECTION_ COULD_NOT_BE_OPENED (11751) Type: communicationsAlarm Package: racloms.OMS_FILE_TRANSFER_ CONNECTION_COULD_NOT_BE_OPENED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: OMS FILE TRANSFER CONNECTION COULD NOT BE OPENED Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: OMS FILE TRANSFER CONNECTION COULD NOT BE OPENED\n\nStarting of a new file transfer connection has failed.\n\nFile transfer between the OMS and a target network element is not working.\n\nAlarm will be cleared automatically by the alarm system after its lifetime has expired. This alarm has a lifetime of 10 minutes.		
Remedial action: The error can be caused by many different reasons (configuration error, for example a faulty IP address, out of memory, load is too high, and so on). Follow the steps to find out the reason for the error:\n\n1. Open web browser.\n\n2. Go to page https://<OMS IP address>/\n\n3. Select "Element Manager Login" and open Log Viewer.\n\n4. Check the log for errors.\n\nIf the problem persists, see the troubleshooting documentation for how to fix the problem. If that does not provide a solution, contact the local Nokia representative.		

Table 41-182 OMS_MEASUREMENT_DATA_PROCESSING_OVERLOAD

Alarm	Attributes	Applicable major release
Name: OMS_MEASUREMENT_DATA_ PROCESSING_OVERLOAD (11752) Type: qualityOfServiceAlarm Package: racloms.OMS_MEASUREMENT_DATA_ PROCESSING_OVERLOAD Raised on class: racloms.OMS	Severity: indeterminate Specific problem: OMS MEASUREMENT DATA PROCESSING OVERLOAD Implicitly cleared: true Default probable cause: SYSTEM_RESOURCES_ OVERLOAD	Release: • LOMS16A
Description: OMS MEASUREMENT DATA PROCESSING OVERLOAD\n\nThe time used for processing performance measurement data in OMS has exceeded the defined limit. This does not necessarily indicate any loss of measurement data but the measurement parameters should be changed to decrease load and prevent possible problems caused by the overload.\n\nThe limits used to set and cancel this alarm can be changed by the user from OMS LDAP parameters.\n\nToo much measurement data is produced in the network elements and OMS overload causes a risk for losing some data.\n\n-		
Remedial action: Do not clear the alarm. Alarm System will clear the alarm after data processing load decreases to normal level.		

Table 41-183 OPERATING_SYSTEM_MONITORING_FAILURE

Alarm	Attributes	Applicable major release
Name: OPERATING_SYSTEM_MONITORING_ FAILURE (11753) Type: processingErrorAlarm Package: racloms.OPERATING_SYSTEM_ MONITORING_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: OPERATING SYSTEM MONITORING FAILURE Implicitly cleared: true Default probable cause: SYSTEM_CALL_ UNSUCCESSFUL	Release: • LOMS16A

Table 41-183 OPERATING_SYSTEM_MONITORING_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: OPERATING SYSTEM MONITORING FAILURE\n\nThe fault detector in the operating system has failed to capture the statistics of the usage of a given resource.\n\nThe state of the named device cannot be discovered, which may indicate that there are some fundamental problems with it.\n\nDo not clear the alarm. The alarm is automatically cleared when the fault detector of the operating system is able to capture the statistics of the failed resource..		
Remedial action: If the alarm is not cleared automatically, contact your local customer support.		

Table 41-184 ORACLE_CLUSTER_ALERT

Alarm	Attributes	Applicable major release
Name: ORACLE_CLUSTER_ALERT (11754) Type: processingErrorAlarm Package: racloms.ORACLE_CLUSTER_ALERT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ORACLE CLUSTER ALERT Implicitly cleared: false Default probable cause: APPLICATION_ SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: ORACLE CLUSTER ALERT\n\nAlerts are generated for different types of problem or failure regarding Automatic Storage Management, Oracle Clusterware or Oracle Database Instance. Examine the alert log and Oracle documentation(from Oracle website) for additional information. There might be different alarms for different database instances and alert log files.\n\nThe effect varies for different problems or failures. Please refer to the Oracle documentation to identify the severity of the problem.\n\nThis alarm does not automatically clear since there is no automatic way of determining when the problem has been resolved..You will need to clear the alarm manually with alarm management application once the problem is fixed.		
Remedial action: Check alarms and alert logs that occurred before this alarm was raised; check the Oracle documentation for advice according to error code and symptom. Alternatively, you can contact your local NSN representative and provide the information you obtained (alarm notification's fields and alert logs). \nThe following alert log files can be found in database node:\n${ORACLE_BASE}/admin/<ORACLE_DB_NAME>/bdump/alert_<ORACLE_SID>.log\n${ORACLE_BASE}/admin/+ASM/bdump/alert_<ASM_SID>.log\n${ORA_CRS_HOME}/log/$(hostname)/alert<hostname>.log		

Table 41-185 ORACLE_CLUSTER_ASM_GROUP_IS_GETTING_FULL

Alarm	Attributes	Applicable major release
Name: ORACLE_CLUSTER_ASM_GROUP_IS_ GETTING_FULL (11755) Type: processingErrorAlarm Package: racloms.ORACLE_CLUSTER_ASM_ GROUP_IS_GETTING_FULL Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ORACLE CLUSTER ASM GROUP IS GETTING FULL Implicitly cleared: true Default probable cause: STORAGE_CAPACITY_ PROBLEM_M3100	Release: • LOMS16A
Description: ORACLE CLUSTER ASM GROUP IS GETTING FULL\n\nOracle cluster ASM (automatic storage management) is reaching the space limit.\n\nOracle database instance might prevent adding or updating data because it is running out of disk space.\n\nThe system clears the alarm automatically when the fill ratio of Automatic Storage Management is below the threshold limit.		
Remedial action: Clean up obsolete data or add a new storage device. In the latter case check the Oracle documentation for instructions on adding new disks.\nAlternatively, increase the value of the fsdbFillRatioAlarmLimit attribute of the Oracle database in the LDAP fsdbFragement if the free space is sufficiently large. The Oracle watchdog will need to be restarted in order to make it aware of the change to the threshold limit.		

Table 41-186 ORACLE_CLUSTER_COMPONENT_IS_FAULTY

Alarm	Attributes	Applicable major release
Name: ORACLE_CLUSTER_COMPONENT_IS_FAULTY (11756) Type: processingErrorAlarm Package: racloms.ORACLE_CLUSTER_COMPONENT_IS_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: ORACLE CLUSTER COMPONENT IS FAULTY Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: ORACLE CLUSTER COMPONENT IS FAULTY\n\nOne or more Oracle database server component(s) become unexpectedly unavailable, such as one Oracle database instance or listener is down. There might be more than one different alarm, e.g. different database instance.\n\nThe effect may be various depending on the severity of the failure. In addition, Oracle Real Application Clusters has got its own high availability, so it might recover from the fault by itself, later. The worst situation is that all the Oracle database services are unavailable because all database instances are unavailable.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Issue crs_stat to check the status of the Oracle cluster database, and check the Oracle alert logs on the faulty node for the errors issued by the Oracle server. In addition look at events that occurred before this alarm was raised. You can alternatively contact your local NSN representative and provide the information you obtained (alarm notification's fields and alert logs).		

Table 41-187 O_M_MEDIATION_FAILURE

Alarm	Attributes	Applicable major release
Name: O_M_MEDIATION_FAILURE (11757) Type: communicationsAlarm Package: racloms.O_M_MEDIATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: O&M MEDIATION FAILURE Implicitly cleared: true Default probable cause: COMMUNICATION_PROTOCOL_ERROR	Release: • LOMS16A
Description: O&M MEDIATION FAILURE\n\nNWI3 connection problem between OMS and NetAct.\n\nThis alarm is set by OMS unit when WBTS O&M operation reply sending from OMS to NetAct has failed.\n\nIn case of NWI3 problem the WBTS O&M mediation tasks done by OMS unit cannot be performed (SW download, SW version upload, HW configuration upload).\n\nDo not clear the alarm. This alarm is cancelled automatically by the system.\n\nAfter the problem in NWI3 connection has been corrected, the system will cancel the alarm only when the next O&M mediation event is successfully sent to NetAct. Thus it is normal behavior that alarm stays active for a while after the problem has been corrected.		
Remedial action: No actions required from the operator.		

Table 41-188 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • LOMS16A
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		

Table 41-188 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 41-189 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • LOMS16A
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 41-190 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • LOMS16A
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 41-191 PLUG_IN_UNIT_FAILURE

Alarm	Attributes	Applicable major release
Name: PLUG_IN_UNIT_FAILURE (11758) Type: equipmentAlarm Package: racloms.PLUG_IN_UNIT_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PLUG-IN UNIT FAILURE Implicitly cleared: false Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: PLUG-IN UNIT FAILURE\n\nA fatal failure in the plug-in unit hardware has been detected.\n\nThere is a severe fault in the plug-in unit hardware. This may cause, for example, the plug-in unit to be automatically shut down by the hardware management to prevent physical damage to it.\n\nClear the alarm with alarm management application after correcting the fault as presented in Instructions.		
Remedial action: Replace the plug-in unit. Note that replacing an operational disk drive may cause loss of data.\n\nDetails of the faulty plug-in unit are found in the Application Additional Info field of the alarm (cabinet, chassis and slot).		

Table 41-192 PLUG_IN_UNIT_TEMPERATURE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: PLUG_IN_UNIT_TEMPERATURE_OUT_OF_ LIMIT (11759) Type: equipmentAlarm Package: racloms.PLUG_IN_UNIT_TEMPERATURE_ OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PLUG-IN UNIT TEMPERATURE OUT OF LIMIT Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: PLUG-IN UNIT TEMPERATURE OUT OF LIMIT\n\nThe reading of a single IPMI (Intelligent Platform Management Interface) temperature sensor is out of limit.\n\nIf the alarm is set off constantly, there is a severe temperature-related problem and the plug-in unit may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check that the air flows freely through the cabinet and the chassis. \n\n2. If the alarm is persistent, replace the faulty plug-in unit. \n\n Refer to the hardware maintenance documentation for detailed replacing\n instructions.\n\n3. If there are numerous alarms of this kind from several plug-in units, check the air conditioning and temperature in the network element (NE) equipment room.\n\nThe details of the faulty plug-in unit (cabinet, chassis and slot) are found in the Application Additional Info field of the alarm.		

Table 41-193 PLUG_IN_UNIT_VOLTAGE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: PLUG_IN_UNIT_VOLTAGE_OUT_OF_LIMIT (11760) Type: equipmentAlarm Package: racloms.PLUG_IN_UNIT_VOLTAGE_OUT_ OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PLUG-IN UNIT VOLTAGE OUT OF LIMIT Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: PLUG-IN UNIT VOLTAGE OUT OF LIMIT\n\nThe reading of a single IPMI (Intelligent Platform Management Interface) voltage sensor is out of limit.\n\nIf the alarm is set off constantly, there is a severe hardware problem and the plug-in unit may behave unexpectedly.\n\nThe system clears the alarm automatically when the fault has been corrected.		

Table 41-193 PLUG_IN_UNIT_VOLTAGE_OUT_OF_LIMIT (continued)

Alarm	Attributes	Applicable major release
Remedial action: 1. Verify the network element (NE) power supply by checking if there are any alarms from the power entry modules of the chassis. \n\n2. Check that the power failure is limited to a single plug-in unit. \n\n3. If the alarm is not automatically cancelled within 20 minutes or there are other indications of plug-in unit power failures, replace the plug-in unit.\n\nRefer to the hardware maintenance documentation for detailed replacing\ninstructions.\n\nThe details of the faulty plug-in unit (cabinet, chassis and slot) are found in the Application Additional Info field of the alarm.		

Table 41-194 PM_FTP_CONNECTION_FAILED

Alarm	Attributes	Applicable major release
Name: PM_FTP_CONNECTION_FAILED (11761) Type: communicationsAlarm Package: racloms.PM_FTP_CONNECTION_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PM FTP CONNECTION FAILED Implicitly cleared: true Default probable cause: COMMUNICATION_ PROTOCOL_ERROR	Release: • LOMS16A
Description: PM FTP CONNECTION FAILED\n\nFile transfer operation failed when trying to upload measurement file from a network element to OMS. IP-address in the additional information field tells which interface the problem concerns.\n\nThis alarm will not be set immediately after a file transfer operation fails, but only after the file transfer has failed to the same IP-address consequently over the duration defined by LDAP parameter OMS/OMSRNC/SS_RNCPM/OMSMeaHandler/BTSFTPAlarmSetDelay.\n\nMeasurement data may be lost or delayed.\n\n-		
Remedial action: Normally the alarm does not need to be cleared but the system cancels the alarm automatically when the file transfer operation is successful. However, if the related network element is removed altogether from the network or its IP-address is changed, it may be necessary to cancel the alarm manually using Element Manager.		

Table 41-195 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 41-196 POSSIBLE_SECURITY_THREAT_IN_NETWORK_ELEMENT

Alarm	Attributes	Applicable major release
Name: POSSIBLE_SECURITY_THREAT_IN_NETWORK_ELEMENT (11762) Type: qualityOfServiceAlarm Package: racloms.POSSIBLE_SECURITY_THREAT_IN_NETWORK_ELEMENT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: POSSIBLE SECURITY THREAT IN NETWORK ELEMENT Implicitly cleared: false Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: POSSIBLE SECURITY THREAT IN NETWORK ELEMENT\n\nThere is reason to suspect that someone is trying to intrude a network element. This condition emerges if there are too many subsequent failed login attempts.\n\nSomeone may be trying to intrude a network element.\n\nClear the alarm with the alarm management application after correcting the fault.		
Remedial action: Security log data must be checked - /var/log/auth.log. Specially investigate the login entries that were made just before the alarm was raised. Check information about account name that was accessed and source address of possible attack.		

Table 41-197 POWER_SUPPLY_FAILURE

Alarm	Attributes	Applicable major release
Name: POWER_SUPPLY_FAILURE (11763) Type: equipmentAlarm Package: racloms.POWER_SUPPLY_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: POWER SUPPLY FAILURE Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: POWER SUPPLY FAILURE\n\nThere is a failure in one of the power modules.\n\nIf all power entry modules are down, the result is degraded chassis power supply redundancy or total loss of power.\n\nDo not clear the alarm. The system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check the power supply voltages to the chassis. Switch on the power entry module circuit breaker if operated. Check the chassis power enable switch. Replace the faulty power module.		

Table 41-198 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • LOMS16A
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 41-199 PROCESSING_OF_ALARMS_IS_STARTED_ANEW

Alarm	Attributes	Applicable major release
Name: PROCESSING_OF_ALARMS_IS_STARTED_ANEW (11764) Type: communicationsAlarm Package: racloms.PROCESSING_OF_ALARMS_IS_STARTED_ANEW Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PROCESSING OF ALARMS IS STARTED ANEW Implicitly cleared: true Default probable cause: COMMUNICATION_PROTOCOL_ERROR	Release: • LOMS16A
Description: PROCESSING OF ALARMS IS STARTED ANEW\n\nA centralised part of the alarm system, functioning in an active\nmaintenance computer, has become active in such a way that it is\nstarting the processing of the alarms of the network element in\nquestion from the beginning. This situation occurs when the system\nrestarts, and as a result of an uncontrolled maintenance computer\nswitchover.\n\nAlarm upload to NetAct is starting.\n\nAlarm is cleared automatically after Time-to-Live expires.		
Remedial action: The alarm requires no actions.		

Table 41-200 PROCESS_START_UP_FAILED_DUE_TO_AN_UNAVAILABLE_SERVICE

Alarm	Attributes	Applicable major release
Name: PROCESS_START_UP_FAILED_DUE_TO_AN_UNAVAILABLE_SERVICE (11765) Type: processingErrorAlarm Package: racloms.PROCESS_START_UP_FAILED_DUE_TO_AN_UNAVAILABLE_SERVICE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: PROCESS START-UP FAILED DUE TO AN UNAVAILABLE SERVICE Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_UNAVAILABLE	Release: • LOMS16A
Description: PROCESS START-UP FAILED DUE TO AN UNAVAILABLE SERVICE\n\nA service required for the application's functionality is unavailable.\n\nDepending on the alarm severity, an application's start-up or run-time session can either fail (CRITICAL severity) or partially lose functionality (MAJOR severity).\n\nThe alarm will be cleared automatically by the alarm system after five minutes. If the service is still unavailable, the alarm is raised again.		
Remedial action: 1. Observe the application dependent on the service by checking the "Application Id" field of the alarm.\n \n2. Observe the service in question by checking the "Managed Object" field of the alarm that contains the service's recovery group (RG).\n\n3. Lock the application in case of a CRITICAL severity alarm to prevent its infinite restart by using the command:\n\nfshascli -l <Application Id>\n\n4. Follow the troubleshooting instructions found in customer documentation for the application in question and try to repair the service. For example, a service can be locked by high availability services (HAS) and its recovery assumes unlocking of the service.\n\n5. Check for any potential alarm(s) for the service in the list of active ones. The corresponding alarm manual(s) describe recovery actions for the service.\n\n6. Check the troubleshooting instructions in the service customer documentation.\n\n7. If the service was successfully recovered, unlock (if the third step was used) the application with the following command:\n\nfshascli -u <Application Id>\n\n8. If the previous steps cannot resolve the situation, contact your local Nokia representative.		

Table 41-201 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • LOMS16A

Table 41-201 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 41-202 RAID_ARRAY_HAS_BEEN_DEGRADED

Alarm	Attributes	Applicable major release
Name: RAID_ARRAY_HAS_BEEN_DEGRADED (11766) Type: equipmentAlarm Package: racloms.RAID_ARRAY_HAS_BEEN_DEGRADED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RAID ARRAY HAS BEEN DEGRADED Implicitly cleared: true Default probable cause: DISK_PROBLEM	Release: • LOMS16A
Description: RAID ARRAY HAS BEEN DEGRADED\n\nRedundancy of the RAID array is lost. A device belonging to the RAID array can be marked faulty by the system. The alarm may be caused by either errors in the fibre channel (FC) or small computer system interface (SCSI) bus or by a potentially broken disk media.\n\nIn the case of a subsequent disk failure, data will be lost.\n\nThe alarm is automatically cleared by the operating system's fault detector once the redundancy of the RAID array is restored.		
Remedial action: If the hardware is FlexiServer Blade Hardware, then follow these instructions:\n1. Use the command cat /proc/mdstat to check the status of the RAID array found in the Identifying additional information field of the alarm on the node that reports the alarm. \nThe [UU] field printed by the command describes whether both of the disks are in the RAID array or not. If this field contains [_U] or [U_], one of the disks is not in the RAID array.\n2. The redundancy of the RAID array should be automatically restored by the system within an hour. If the problem persists and the alarm is not cleared within an hour, contact your local Nokia representative.\n3. If the problem persists, try changing the faulty disk according to the hardware maintenance instructions. If that does not help, contact your local Nokia representative.\n\nIf the hardware is IBM BladeCenter, then follow these instructions:\n1. Check the Maintenance Module and find the faulty Disk and the possible cause of the fault. Replace the faulty disk with a new disk, referring to the hardware maintenance documentation for detailed replacement instructions.\n2. The redundancy of the RAID array should be automatically restored by the system within an hour. If the problem persists and the alarm is not cleared within an hour, contact your local Nokia representative.		

Table 41-203 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • LOMS16A

Table 41-203 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 41-204 ReconfigFailure

Alarm	Attributes	Applicable major release
Name: ReconfigFailure (1949) Type: communicationsAlarm Package: netw.ReconfigFailure Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: failedReconfig	Release: • LOMS16A
Description: This alarm is raised when the reconfig action failed.		
Raising condition: ('State' EQUAL 'Failed')		
Clearing condition: ('State' NOT EQUAL 'Failed')		
Remedial action: Verify that the object is configured as expected.		

Table 41-205 RECOVERY_ACTIONS_BANNED_FOR_MANAGED_OBJECT

Alarm	Attributes	Applicable major release
Name: RECOVERY_ACTIONS_BANNED_FOR_ MANAGED_OBJECT (11767) Type: processingErrorAlarm Package: racloms.RECOVERY_ACTIONS_BANNED_ FOR_MANAGED_OBJECT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RECOVERY ACTIONS BANNED FOR MANAGED OBJECT Implicitly cleared: true Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A

Table 41-205 RECOVERY_ACTIONS_BANNED_FOR_MANAGED_OBJECT (continued)

Alarm	Attributes	Applicable major release
Description: RECOVERY ACTIONS BANNED FOR MANAGED OBJECT\n\nAn operator has set the specified managed object to an inert mode. The managed object identifies a node. If the inert mode is set for the whole cluster, this alarm is raised separately for each node. \nWhile the inert mode is on, high availability services (HAS) does not attempt to recover services from failures, for example, by restarting nodes or applications, or by performing switchovers within the specified managed objects. Note that the inert mode should be used only by qualified supplier's representatives when analysing problems in the system.\nThe inert mode is switched on by issuing an fshascli command, for example:\n$ fshascli --inert-mode on /CLA-0\nThe command above switches the inert mode on for the /CLA-0 node. Accordingly, the inert mode can be switched off by using the fshascli command:\n$ fshascli --inert-mode off /CLA-0\n\nThis alarm is raised when an operator switches the inert mode on for either a set of nodes or the cluster.\nThe inert mode has the following effects on the behaviour of the system in nodes for which the inert mode has been switched on:\n - If there are no failures, the service provided by the network element is not affected.\n - If failures occur, no recovery actions are performed and the service may be affected. For example, if a process fails, it is not restarted by HAS.\n - Process failures are still propagated to the recovery unit level, but the recovery unit level fault recovery does not take place. In practice, this means that the propagated process failure does not cause restarts of other recovery unit processes, and switchovers do not take place with active/standby recovery groups.\n - HAS logs pending recovery actions to master syslog (/var/log/master-syslog on the active CLA node) in the form 'INFO Inert mode set for <managed object name>. Recovery action \'restart\' pending.'.\n - HAS does not raise any alarms for managed objects in the inert mode. The inert mode for a node sets all managed objects within the node to the inert mode.\n - The inert mode sustains in the nodes over node or cluster restarts.\n - Only the node and cluster restart, power on and power off fshascli commands work while the inert mode is set for the nodes or the cluster.\nNote that fault recovery in the nodes that are not in the inert mode works normally.\n\nThe system clears the alarm when the inert mode is switched off from the managed object.		
Remedial action: 1. To ensure proper functionality of the system, switch off the inert mode after the problem analysis is done. \n2. You can switch off the inert mode from all nodes of the cluster by issuing the fshascli command:\n$ fshascli --inert-mode off /\nNote that this should be done by the supplier's field engineer that is currently analysing the system. \nWhen the inert mode is switched off, pending recovery actions take place. For example, if an important severity process in a cold active/standby recovery group has failed in a node that was in the inert mode, switching the inert mode off for the node causes a switchover of the recovery group.		

Table 41-206 RECOVERY_GROUP_SWITCHOVER

Alarm	Attributes	Applicable major release
Name: RECOVERY_GROUP_SWITCHOVER (11768) Type: processingErrorAlarm Package: racloms.RECOVERY_GROUP_ SWITCHOVER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RECOVERY GROUP SWITCHOVER Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ ABNORMALLY_TERMINATED	Release: • LOMS16A
Description: RECOVERY GROUP SWITCHOVER\n\nThe platform high availability services (HAS) has initiated a switchover. This may be a recovery action to a recovery unit (RU) failure or result from an administrative operation such as lock or shutdown of the active RU or a switchover request from an explicit recovery group (RG). The new active recovery use is now starting (a cold active standby RG) or being activated (a hot active standby RG).\n\nThe service provided by the RG is currently unavailable. The normal operation will resume if the switchover operation is successful.\n\nThe alarm system will clear the alarm automatically after the problem is solved (the switchover succeeds).		

Table 41-206 RECOVERY_GROUP_SWITCHOVER (continued)

Alarm	Attributes	Applicable major release
Remedial action: Verify that the switchover operation is successful. This alarm is automatically cleared if the switchover succeeds. However, depending on the type of the application, the time for starting (or activating) a standby RU can vary from a few seconds to tens of minutes. The state of the new active RU can be checked using the HAS user interface fshascli: \n\n1. Log into the cluster.\n2. Use the fshascli -s option to see the state of the new active RU. The MO name of the new active RU can be found in the application additional information field 1.\nFor example, execute the following command to check the state of the fictitious /AS-10/ApplServer-0 recovery unit: \nfshascli -s /AS-10/ApplServer-0 \n\nAn operational RU has UNLOCKED administrative state, ENABLED operational state, an empty procedural status, and "ACTIVE" role. The procedural status of INITIALIZING means that the RU is still starting up. If the switchover fails (operational state of the new active RU is DISABLED), check the syslog for a possible explanation for the failure and if required, contact your Nokia representative. \n\nNote that if both RUs in the active standby RG fail repeatedly, this alarm may be raised for both RUs. In that case the situation has to be corrected immediately.		

Table 41-207 RECREATING_STANDBY_IN_MEMORY_DATABASE_FAILED

Alarm	Attributes	Applicable major release
Name: RECREATING_STANDBY_IN_MEMORY_DATABASE_FAILED (11769) Type: processingErrorAlarm Package: racloms.RECREATING_STANDBY_IN_MEMORY_DATABASE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RECREATING STANDBY IN-MEMORY DATABASE FAILED Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: RECREATING STANDBY IN-MEMORY DATABASE FAILED\n\nThe watchdog process failed to copy the database from the active database to standby at start-up, either after switchover or after failover.\n\nThe standby database does not exist any more or contains out-of-date data. High availability of the database cannot be guaranteed. Typically, the active database raises the alarms 70205 and 71065 because the standby database replication agents are not functional.\n\nThe alarm is cleared automatically by the watchdog process when recreating finally succeeds.		
Remedial action: If the reason for the failure is SyncError, \n1. Get the recovery unit name of the peer watchdog by using the command\nfshascli -v / | grep '^RecoveryUnit.*InMemoryDB'\nThe correct recovery unit is the one that has the prefix /<node>, where <node> is the peer node name in the additional information field #2.\n2. Check the status of the recovery unit with the command\nfshascli -s <RU name>\n3. If the administrative state of the recovery unit is LOCKED, unlock the recovery unit with the command\nfshascli -LN <RU name>\n4. If the problem does not disappear, contact your Nokia representative and provide them with the information in the alarm notification and the results of the actions described above.\nIn other cases contact your Nokia representative and provide them with the information in the alarm notification and system log.		

Table 41-208 RegistrationServiceConfiguration

Alarm	Attributes	Applicable major release
Name: RegistrationServiceConfiguration (11773) Type: configurationAlarm Package: racloms.RegistrationServiceConfiguration Raised on class: racloms.OMS	Severity: major Specific problem: Failed to configure the CORBA Registration Service in OMS Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: Failed to configure the CORBA Registration Service in OMS. The additional information of the alarm contains the detail of the error.		

Table 41-208 RegistrationServiceConfiguration (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please refer to the LTE RAN User Guide to know how to manually set the Registration Service in OMS.		

Table 41-209 REPLICATION_FAILING_FOR_IN_MEMORY_DATABASE

Alarm	Attributes	Applicable major release
Name: REPLICATION_FAILING_FOR_IN_MEMORY_DATABASE (11770) Type: processingErrorAlarm Package: racloms.REPLICATION_FAILING_FOR_IN_MEMORY_DATABASE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: REPLICATION FAILING FOR IN-MEMORY DATABASE Implicitly cleared: true Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: REPLICATION FAILING FOR IN-MEMORY DATABASE\n\nReplication for the in-memory database is not functioning.\n\nUpdates from the active to the standby database are not replicated. The standby database cannot become active (no successful failover for database application) unless replication starts functioning again (or the database is copied from the active node as a part of start-up or switchover recovery).\n\nLog files may not be purged; this may eventually fill the database disk partition making further updates to the database impossible.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. See the reason for the failure from field 1 of the application additional info.\n\n2. If the reason is "NoReplication-Agent" the watchdog process attempts to restart the agent automatically after raising the alarm. Use the parameter management application to check the value of fsdbReplicationStatusCheckInterval attribute. The value defines how often the watchdog checks the status of the replication. Wait until the next status check takes place. If the alarm still remains in the active alarms list, copy the current contents of syslog and give item to your local Nokia representative.\n\n3. If the reason is "ReplicationStopped" somebody has stopped the replication typically intentionally. The watchdog process does not attempt to restart the replication automatically. The replication must be restarted manually with the command\nttAdmin -repStart <DB-name>\nIf the alarm does not go away from or re-appears soon the active alarm list, copy the current contents of syslog and contact your local Nokia representative.\n\n4. If the reason is "ReplicationFallenBehind", the database instance having active role is not able to keep the standby database synchronised as required by the fsdbReplicationStatusCheckLimit attribute. Typically, one of the two nodes running peer database instances or network is overloaded when this alarm is raised. A peak in transaction flow produced by the database applications may also cause this alarm.\nIf this alarm persists in the active alarms list, use top and ifconfig tools to estimate the current load in your system and contact your local Nokia representative.\n\n5. If the reason is "CommunicationProblem" use\nfshascli -s /<node>/<RU-name>\nto verify that the status of the peer in-memory database recovery unit (<node> is of the 3 from application additional info and that the<RU-name> can be derived from the Application field of the alarm). If the peer recovery unit is locked, unlock it with the command\nfshascli -u /<node>/<RU-name>\nIf the alarm still persists , copy the current contents of syslog and contact your local Nokia representative.		

Table 41-210 RESOURCE_ALLOCATION_OR_DE_ALLOCATION_FAILURE

Alarm	Attributes	Applicable major release
Name: RESOURCE_ALLOCATION_OR_DE_ALLOCATION_FAILURE (11771) Type: processingErrorAlarm Package: racloms.RESOURCE_ALLOCATION_OR_DE_ALLOCATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RESOURCE ALLOCATION OR DE-ALLOCATION FAILURE Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ABNORMALLY_TERMINATED	Release: • LOMS16A

Table 41-210 RESOURCE_ALLOCATION_OR_DE_ALLOCATION_FAILURE (continued)

Alarm	Attributes	Applicable major release
Description: RESOURCE ALLOCATION OR DE-ALLOCATION FAILURE\n\nAllocation or deallocation of resources to or from a computer node in the cluster has failed. Applications running in the cluster are often identified with resources that are allocated to the node before the application is started and released from the node, and after the application has terminated. Such resources can, for example, be TCP/IP addresses that are associated with the service provided by the software, or a disk partition that, for example, contains the application database. In addition, the application can allocate and deallocate other resources (for example, start and stop 3rd party applications) in its control scripts. An operation failure has been reported for the defined recovery unit, while it was starting or stopping.\n\nIf the error occurred when an application was starting, application start-up is aborted. In case of a permanent fault, the service provided by the application is now down. With a transient or node-specific fault, and provided that the application has a standby resource, the application may have been restarted successfully on another node. If the fault happened while the application was terminating, the node on which the error happened has now been restarted to restore it to a known state. If the node has restarted successfully or the application has a standby resource, the application has likely already restarted, and service is again available.\n\nThe system automatically clears the alarm when the fault has been corrected.		
Remedial action: 1. Log in to the network element as root user to check the situation. \n\n2. Use the fshascli command to check the state of all recovery units within the recovery group (the name of the recovery group is in the Application Additional Information field). If the recovery group is providing service, each of its UNLOCKED recovery unit that has the ACTIVE role has the ENABLED operational state, and an empty procedural status. For example, the state of recovery units of the /Directory recovery groups can be checked as follows: \n$ fshascli -se Directory --filter ru\n/CLA-0/FSDirectoryServer:\nadministrative(UNLOCKED)\noperational(ENABLED)\nusage(IDLE)\nprocedural(NOTINITIALIZED)\navailability()\nunknown(FALSE)\nalarm()\nnrole(COLDSTANDBY)\n\n/CLA-1/FSDirectoryServer:\nadministrative(UNLOCKED)\noperational(ENABLED)\nusage(ACTIVE)\nprocedural()\navailability()\nunknown(FALSE)\nalarm()\nrole(ACTIVE)\n\nIn the case above, the recovery unit of the CLA-0 node is acting as a cold standby backup, and the recovery unit on CLA-1 is running the service normally. Note that the grep command in the example is used to filter out information regarding individual processes in each recovery unit. \n\nSince this is a situation that may be caused by various faults, contact your Nokia representative to analyze the root-cause.		

Table 41-211 RUIMRMEX_LDAP_DATA_DISTRIBUTION_FAILURE

Alarm	Attributes	Applicable major release
Name: RUIMRMEX_LDAP_DATA_DISTRIBUTION_FAILURE (11772) Type: communicationsAlarm Package: racloms.RUIMRMEX_LDAP_DATA_DISTRIBUTION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: RUIMRMEX LDAP DATA DISTRIBUTION FAILURE Implicitly cleared: false Default probable cause: REMOTE_NODE_TRANSMISSION_ERROR	Release: • LOMS16A
Description: RUIMRMEX LDAP DATA DISTRIBUTION FAILURE\n\nIn the Manager side: Reading RUIM related external NetAct LDAP access data from the manager node's LDAP server or sending it to resource side failed.\n\nIn the Resource side: Writing RUIM related external NetAct LDAP access data to the resource node's LDAP server failed.\n\nA NetAct RUIM user cannot access a resource network element since that resource node has wrong RUIM related external NetAct LDAP access configuration data.\n\nClear the alarm with alarm management application after correcting the fault as presented in Instructions.		
Remedial action: Alarm reported in Manager side: check that \n1) the network connection to the resource node in question is working\nCorrection: Repair the network connection.\n2) the resource node in question, or the RUEM RMEX RG in it, are up and running\nCorrection: Reboot the node or the RUEM RMEX RG.\n3) the access to the node's LDAP server is allowed\nCorrection: Check that the node's LDAP server is up and running OR that the credentials used for the local LDAP access are correct.\n\nAlarm reported in the Resource side: check that \n1)the access to the node's LDAP server is allowed\nCorrection: Check that the node's LDAP server is up and running OR that the credentials used for the local LDAP access are correct.		

Table 41-212 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • LOMS16A
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 41-213 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 41-214 SERVICE_LEVEL_DEGRADED_BELOW_THRESHOLD

Alarm	Attributes	Applicable major release
Name: SERVICE_LEVEL_DEGRADED_BELOW_ THRESHOLD (11774) Type: equipmentAlarm Package: racloms.SERVICE_LEVEL_DEGRADED_ BELOW_THRESHOLD Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SERVICE LEVEL DEGRADED BELOW THRESHOLD Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A

Table 41-214 SERVICE_LEVEL_DEGRADED_BELOW_THRESHOLD (continued)

Alarm	Attributes	Applicable major release
Description: SERVICE LEVEL DEGRADED BELOW THRESHOLD\n\nThe number of active recovery units within the load sharing group has dropped below the predefined threshold. This can happen because of \n\n1) management actions (number of recovery units or nodes have been locked),\n2) a series of node failures or\n3) continuous failure to restart the recovery unit(s) within the load sharing group.\n\nThe alarm is informative by nature and it indicates that the load sharing group cannot maintain the acceptable service level.\n\nDo not clear the alarm. The system clears the alarm automatically when the number of operational RUs goes above the defined threshold.		
Remedial action: The alarm does not require any particular corrective actions if it is preceded by either deliberate management action(s) or node failures. In the latter case separate alarms indicating the node failures would have been raised. \n\nIf, however, the reason is that the recovery units have failed and system is not able to restart the software, the problem is in the applications forming the load sharing group. Basically, there could be several reasons why an application cannot be restarted and therefore it is difficult to give exact or detailed instructions on how to deal with the situation. \n\nThe first thing to be checked is the availability statuses of the failed recovery units. If RU's availability status has value failed, system has already attempted to restart it with no success. Note, that it is possible to try to restart the recovery unit also manually with e.g. fshascli -r command. If also manual restarting fails, the log writings should be detected: a typical cause for failing restart might be missing configuration file, incorrect configuration file content or even lack of some critical resources, e.g. the amount of available physical memory.		

Table 41-215 SS7___SIGTRAN_PROTOCOL_STACK_CONFIGURATION_FAILURE

Alarm	Attributes	Applicable major release
Name: SS7___SIGTRAN_PROTOCOL_STACK_CONFIGURATION_FAILURE (11775) Type: processingErrorAlarm Package: racloms.SS7___SIGTRAN_PROTOCOL_STACK_CONFIGURATION_FAILURE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SS7 / SIGTRAN PROTOCOL STACK CONFIGURATION FAILURE Implicitly cleared: false Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A
Description: SS7 / SIGTRAN PROTOCOL STACK CONFIGURATION FAILURE\n\nA protocol \n\n- MTP3-user adaptation layer (M3UA) \n- signalling connection control part (SCCP)\n- transaction capabilities application part (TCAP)\n\nin the SS7/ SIGTRAN stack cannot be started properly due to an initialization\nor configuration problem.\n\nThe SS7/SIGTRAN service is not available, neither SCCP nor TCAP traffic can be sent or received.\n\nClear the alarm with alarm management application after the problem has been corrected as presented in Instructions.		

Table 41-215 SS7___SIGTRAN_PROTOCOL_STACK_CONFIGURATION_FAILURE (continued)

Alarm	Attributes	Applicable major release
Remedial action: See the possible error in the Application Additional Info field and proceed according to the respective procedure.\n\n- AAI_ISS_INIT_NOK: Initialisation of SS7/SIGTRAN stack has failed. \n\n- AAI_SCCP_INIT_NOK: SCCP initialisation has failed. For further information, see the error logs in the syslog.\n\n1. Check the value of SS7 Standard in the SS7/SIGTRAN Load Balancing Service data in the LDAP tree. \n\n2. Check that the value of the fsss7MinSCCPReferenceNbr is lower than the value of the fsss7MaxSCCPReferenceNbr in the configuration data of the process which raised the alarm in the LDAP. \n\n- AAI_GTT_INIT_NOK: Initialisation of GlobalTitleTranslation library has failed. For further information, see the error logs in the syslog.\n \n1. Check the SS7 configuration in the LDAP. \n \n- AAI_TCAP_INIT_NOK: TCAP initialisation has failed. For further information, see the error logs in the syslog. \n\n1. Check the value of SS7 Standard in the SS7/SIGTRAN Load Balancing Service data in the LDAP. \n\n- AAI_M3UA_SCU_NOK: M3UA configuration has failed. For further information, see the error logs in the syslog.\n\n1. Check SS7 configuration in the LDAP. \n\n- AAI_SCCP_SCU_NOK: SCCP configuration has failed. For further information, see the error logs in the syslog. \n\n1. Check the SS7 configuration in the LDAP. \n\n- AAI_TCAP_CONFIG_TRID_NOK: TCAP configuration has failed. For further information, see the error logs in the syslog.\n\n1. Check that the value of the fsss7MinTransactionid is lower than the value of the fsss7MaxTransactionId in the configuration data of the process which raised the alarm in the LDAP.\n\nIf the configuration data is correct but the alarm occurs, contact your Nokia representative and provide them with the information gathered by the following steps:\n\n1. Set tracing on for all protocols in the SS7/Debug fragment (attribute value 1). \n\n2. Change in files /opt/Nokia/SS_SS7LM/script/ss_ss7lm_start.sh and /opt/Nokia/SS_SS7NM/script/ss_ss7nm_start.sh logging on with command: export SS7_LOGOPTS="15\n\n3. Lock the SS7/Sigtran recovery groups (RGs). \n\n4. Unlock the SS7/Sigtran RGs. \n\n5. Check if the following files exist in the node in which the alarm was raised \n /tmp/ss7nmlog.log \n /tmp/ss7lmlog.log \n /tmp/ss7debug.log \n\n6. If the files can be found, copy them and attach them to the problem report. Include in the report also the syslog information from the time the RGs were started."		

Table 41-216 SSL_CONNECTION_CANNOT_BE_MADE_BY_RUIM

Alarm	Attributes	Applicable major release
Name: SSL_CONNECTION_CANNOT_BE_MADE_BY_RUIM (11776) Type: processingErrorAlarm Package: racloms.SSL_CONNECTION_CANNOT_BE_MADE_BY_RUIM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SSL CONNECTION CANNOT BE MADE BY RUIM Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_UNAVAILABLE	Release: • LOMS16A
Description: SSL CONNECTION CANNOT BE MADE BY RUIM\n\nThis alarm indicates that the Remote User Information Management (RUIM) configured to make an SSL connection to the external NetAct LDAP server has failed. \n\nThis alarm is raised due to the following reasons: \n1. The certificate is missing or rejected by the external NetAct LDAP server.\n2. The external NetAct LDAP server is not supporting SSL connections or connections to it cannot be established for any other reason (also see alarm 70268). \n\nNote that, when an SSL connection is attempted but no connection is made because of a connection problem, which is not specific to SSL (for example, wrong IP address), both the alarms 70268 and 70358 are raised. If only the alarm 70358 is raised, then the TLS_OR_PLAIN_TEXT mode is used and the plain text connection has succeeded.\n\nThis alarm indicates that the SSL connection is unsuccessful by RUIM.\nNote that the user will still be able to log in using 'TLS_OR_PLAIN_TEXT' or 'PLAIN_TEXT' modes in RUIM.\n\nThe system clears the alarm automatically when the SSL connection is established with the external LDAP Server.		
Remedial action: Check why SSL connections cannot be made and potentially disable RUIM for the time of investigation (as possible plain-text connections are dangerous). \n\nTo disable RUIM, enter the following command: \n# fscontrolRUIM --disable \n\nDepending on the problem type (see Identifying Application Additional Info) the cause for the problem can be: \n- Certificates are not present in default or RUIM domain\n- Wrong server certificate is used\n- External LDAP does not support SSL protocol		

Table 41-217 STAGING_AREA_IN_INCONSISTENT_STATE

Alarm	Attributes	Applicable major release
Name: STAGING_AREA_IN_INCONSISTENT_STATE (11777) Type: environmentalAlarm Package: racloms.STAGING_AREA_IN_INCONSISTENT_STATE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: STAGING AREA IN INCONSISTENT STATE Implicitly cleared: false Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: STAGING AREA IN INCONSISTENT STATE\n\nInstallation of Incremental Delivery failed, recovery was not performed. Staging Area may be in inconsistent state.\n\nOperator action is needed to perform manual recovery.\n\nOperator shall clear alarm manually after performing manual recovery.		
Remedial action: Operator shall check Nwi3SWAgent logs to determine what caused installation failure. Operator shall use FlexiPlatform Software Management tools or OMS CLI Software Management tools to perform manual recovery.		

Table 41-218 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 41-219 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • LOMS16A
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 41-220 SWITCH_AND_SERVICE_UNIT__FABRIC_BROADCAST_STORM

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT__FABRIC_BROADCAST_STORM (11778) Type: qualityOfServiceAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT__FABRIC_BROADCAST_STORM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: FABRIC BROADCAST STORM Implicitly cleared: true Default probable cause: SYSTEM_RESOURCES_OVERLOAD	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: FABRIC BROADCAST STORM\n\nA broadcast storm control condition has started within the last 250 milliseconds.\n\nThe switch will drop broadcast frames for a fixed period of 250 milliseconds.\n\nThe system clears the alarm automatically.		
Remedial action: No specific actions are required. \n\nHowever, it should be noted that a broadcast storm is traditionally considered as an indication of the existence of a loop in the network. Loops, however, should not be encountered in FlexiServer-based systems since rapid spanning tree protocol (RSTP) is used for blocking the redundant links.\n\nTherefore, if the system does not clear this alarm automatically, it indicates severe error(s) in the elementary system configuration. In this case, handle the alarm as additional debugging information and add it, for example, to a problem report to your local customer support.		

Table 41-221 SWITCH_AND_SERVICE_UNIT__IPMI_SYSTEM_EVENT_LOG_FULL

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT__IPMI_SYSTEM_EVENT_LOG_FULL (11779) Type: qualityOfServiceAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT__IPMI_SYSTEM_EVENT_LOG_FULL Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: IPMI SYSTEM EVENT LOG FULL Implicitly cleared: false Default probable cause: RECUCED_LOGGING_CAPABILITY	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: IPMI SYSTEM EVENT LOG FULL\n\nThe Intelligent Platform Management Interface (IPMI) System Event Log (SEL) is periodically read to /var/log/system.log@<ip address of Switch and Service Unit (SWSE)> file and then cleared by the IPMI event log daemon program, seld. If this alarm appears, the seld program has failed to clear the log.\n\nAny subsequent IPMI event will still be propagated out by the SWSE but they will not be logged in the SEL.\n\nClear the alarm with an alarm management application after correcting the fault as presented in Instructions.		
Remedial action: 1. Check if the seld program is running by executing the following command in the node where the /Directory recovery group is running\n\nps ax | grep -i seld\n\n2. If the seld is running but the log has become full, contact your Nokia representative.\n\n3. If the seld is not running you can try to restart it manually.\n\n/opt/Nokia_BP/bin/seld daemonize\n\n4. If the restart of seld was not successful, read and clear the logs on the switch identified in the alarm. With the -l option you can save the IPMI SEL to a file.\n\nevent -p <IP address of the switch> -d -l log.txt\n\n5. Contact your Nokia representative to find out the root cause for the SEL clearing failure.		

Table 41-222 SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_MEMORY_FULL

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_MEMORY_FULL (11780) Type: qualityOfServiceAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_MEMORY_FULL Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: QUEUE ENGINE MEMORY FULL Implicitly cleared: true Default probable cause: SYSTEM_RESOURCES_OVERLOAD	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: QUEUE ENGINE MEMORY FULL\n\nThe queue engine inside the switch fabric processor has detected that the link memory is full. This is an indication of some level of congestion in the internal communication network.\n\nThe Ethernet switch may not be able to duplicate packets correctly to all the links because the buffer is either full or becoming full. This is not a fatal error, but if the situation is prolonged, for example, because of heavy congestion in the communication network, the switch will have to drop some packets and packet forwarding will be greatly delayed.\n\nThe system will tolerate these disturbances to some extent without noticeable problems. However, if the situation is prolonged, it will eventually cause more severe problems. For example, software will start to report problems in peer-to-peer communication, and in severe cases, the system heartbeats will be lost, which can lead to some software and/or nodes being restarted.\n\nThe alarm system clears the alarm automatically after its time to live has expired.		
Remedial action: No specific actions are required.		

Table 41-223 SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_RESTART

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_RESTART (11781) Type: processingErrorAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT__QUEUE_ENGINE_RESTART Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: QUEUE ENGINE RESTART Implicitly cleared: false Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: QUEUE ENGINE RESTART\n\nThe queue engine inside the switch fabric processor has detected a fatal error, and a queue engine restart has occurred. The switch will not forward traffic before the engine has restarted.\n\nThe fabric processor is restarted. The part of the system using this Ethernet switch experiences a small connectivity break and some data frames are lost. The system will tolerate this. However, other disturbances such as error log writings s from the applications' software will most likely be encountered during the restart. Also, other alarms indicating, for example, network topology change, may be raised.\n\nClear the alarm with an alarm management application after correcting the fault as presented in INSTRUCTIONS.		
Remedial action: 1. Provide your local Nokia representative with the following information:\n\n- the type of the switch blade, its serial number, software version, fabricQueueEngineRestartReason \n\n- information provided by the "show inventory" command:\n\n1. Connect to the switch blade, for example, from the CLA-0 node.\n2. Start the switch management program by issuing the "swc" shell command.\n3. Execute the "show inventory" command.\n\nIn addition to these, provide your local Nokia representative with as much information about the type of applications and traffic patterns in the switch blade prior to the error as possible.		

Table 41-224 SWITCH_AND_SERVICE_UNIT__RSTP_NEW_ROOT

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT__RSTP_NEW_ROOT (11782) Type: equipmentAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT__RSTP_NEW_ROOT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: RSTP NEW ROOT Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: RSTP NEW ROOT\n\nThis switch is now the root for the rapid spanning tree protocol (RSTP) instance.\nThe former root switch blade of the cluster has gone down (or is not accessible\nfor some other reason) forcing this switch blade to be the new root, or this switch blade has come up as a root.\n\nThe altered connectivity topology will most likely cause small disturbances in the communication of the system. Some data frames may be lost or data frame forwarding will be greatly delayed. These disturbances do not affect the functioning of the system.\n\nHowever, other disturbances, such as error log writing from the applications' software will most likely be encountered during the restart. In addition, other alarms indicating, for example, network topology change may be encountered. \n\nNote: Even though this alarm does not indicate that the former root switch has necessarily failed, this alarm would be raised in that situation as well.\n\nThe alarm system clears the alarm automatically after its time to live has expired.		
Remedial action: This alarm does not require any actions.		

Table 41-225 SWITCH_AND_SERVICE_UNIT___RSTP__TOPOLOGY_CHANGE

Alarm	Attributes	Applicable major release
Name: SWITCH_AND_SERVICE_UNIT___RSTP__TOPOLOGY_CHANGE (11783) Type: equipmentAlarm Package: racloms.SWITCH_AND_SERVICE_UNIT___RSTP__TOPOLOGY_CHANGE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH AND SERVICE UNIT: (RSTP) TOPOLOGY CHANGE Implicitly cleared: true Default probable cause: EQUIPMENT_MALFUNCTION	Release: • LOMS16A
Description: SWITCH AND SERVICE UNIT: (RSTP) TOPOLOGY CHANGE\n\nRSTP (rapid spanning tree protocol) has changed the topology of the communication network. Possible reasons are, for example, a switch has crashed or encountered a spontaneous restart, a switch blade might have been replaced or a new switch might have been added to the communication network during a system upgrade.\n\nThe topology change, that is, blocking/unblocking of some links, causes small communication disturbances and in many cases loss of some data frames. The system will tolerate this, but as a symptom, some error logs or other warnings may be encountered momentarily.\n\nDo not clear the alarm. The alarm system clears the alarm automatically after its time to live has expired.		
Remedial action: No specific actions are required.		

Table 41-226 SWITCH_FAULTY

Alarm	Attributes	Applicable major release
Name: SWITCH_FAULTY (11784) Type: communicationsAlarm Package: racloms.SWITCH_FAULTY Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH FAULTY Implicitly cleared: true Default probable cause: LAN_ERROR	Release: • LOMS16A

Table 41-226 SWITCH_FAULTY (continued)

Alarm	Attributes	Applicable major release
Description: SWITCH FAULTY\n\nThe LAN (Local Area Network) monitoring software has declared a switch faulty.\n\nThis is a serious condition as the redundancy level of the system is lowered due to the failed switch.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Check the severity of the alarm. \nIf the severity is WARNING, then:\nThe system is trying to recover the switch and no user actions are needed.\nIf the severity is MAJOR, then:\nIf the "are_resets_enabled" parameter is true in the alarm info,\nthen the system has already tried to reset the switch and the switch must therefore be replaced.\nIf "are_resets_enabled" is off, however, it means that no automatic\nresets have been executed on this switch and manual reset could be beneficial\nas instructed in the hardware maintenance documentation.\nThe name of the switch is included in the application additional info.\n\nRefer to the hardware maintenance documentation for how to change faulty switch.\nAfter replacing the switch and powering it on or restarting it, allow the\nsystem at least five (5) minutes to stabilise the fault information. During\nthat time other alarms might appear and this alarm might be cancelled for\na time but do not react the other alarms.		

Table 41-227 SWITCH_LINK_DOWN

Alarm	Attributes	Applicable major release
Name: SWITCH_LINK_DOWN (11785) Type: equipmentAlarm Package: racloms.SWITCH_LINK_DOWN Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH LINK DOWN Implicitly cleared: true Default probable cause: LINK_FAILURE	Release: • LOMS16A
Description: SWITCH LINK DOWN\n\nA linkDown simple network management protocol (SNMP) trap triggers this alarm. It is an indication that an Ethernet switch port changes from up state to down state.\n\nOnce a port (or link) is in down state, it can't transport any traffic. This is not necessarily an error condition, but this can follow from a maintenance operation such as replacing a cable between two switches, or closing a switch port via management interface. A link may also go to down state if, for example, the host computer or switch at the other end of the link is shut down, restarted, or removed. \n\nHowever, a spontaneous state change may indicate a serious failure, even though the system will typically tolerate these failures to some extent because of redundant networking infrastructure. Note that a linkDown SNMP trap is paired with a linkUp SNMP trap that will trigger a cancelling of the alarm. For example, when replacing a computer node, one would first see the raising of this alarm when the replaced unit is shut down and the automatic cancelling of this alarm when the new blade is taken into use.\n\nThe system automatically clears the alarm when the fault has been corrected.		

Table 41-227 SWITCH_LINK_DOWN (continued)

Alarm	Attributes	Applicable major release
Remedial action: As explained above, this alarm does not typically indicate an error condition, but this relates to other maintenance actions or state changes in the system. However, if there is no clear reason for this alarm and especially if the alarm system does not cancel the alarm automatically within reasonable time (depending on the state of the system), certain corrective actions should be performed.\n\nStart by trying to detect whether the link should be up or not. Note that "link" refers to either hardwired Ethernet connections in the backplane/midplane or Ethernet cables between switches and other devices. During normal operation, all links between active switches and other devices should be up. Try to rule out the possibility that a device at the other end of the link is down because of a power feed failure. For example, in addition, check the administrative statuses of both ends of the link. In a switch, this can be done using the management interface of the switch.\n\nIdentify the link from the management interface. Check from the system logs. And from the current configuration of the switch if, for example, a configuration change or an incorrect configuration has forced the link to a down state. Refer to the documentation provided by the switch manufacturer, if necessary. \n\nIn a host computer, check the network connectivity. In Linux based systems, you can use the command "ethtool <INTERFACE>" to get information from a physical layer of the interface connected to a switch. Use the command "man ethtool" to get help and usage information. If both devices are up and running and their administrative states indicate that they should be able to connect, the next probable cause of a link being down is a loose cable. Check for a bad connectivity, especially if "link" refers to a cable. Even in a case of a backplane/midplane link, check that all relevant blades are firmly and correctly placed in their slots. If connectivity seems to be OK, try rebooting the connected devices. \n\nIf this does not help and the system does not cancel the alarm, try to replace the components:\n\n1. First replace the cable. Note that even in a case of a backplane/midplane link it is possible that the signal wires are broken. However, this is highly unlikely. Backplane failure and backplane replacement should be only considered as the last resort.\n\n2. Next, if the other device is a CPU blade, replace that. Visually inspect the condition of both backplane connectors and the blade connectors: a twisted or broken connector pin can easily cause symptoms such as lost connectivity.\n\n3. As the last option (excluding replacing the chassis backplane as explained above), replace the switch.		

Table 41-228 SWITCH_RESTARTED

Alarm	Attributes	Applicable major release
Name: SWITCH_RESTARTED (11786) Type: equipmentAlarm Package: racloms.SWITCH_RESTARTED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SWITCH RESTARTED Implicitly cleared: false Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A
Description: SWITCH RESTARTED\n\nThe alarm is triggered by a coldStart Simple Network Management Protocol (SNMP) trap sent by an Ethernet switch. The coldStart trap signifies that the sending protocol entity is reinitializing itself and that the management agent's configuration or the protocol entity implementation may have been altered. The warmStart trap signifies that the sending protocol entity is reinitializing itself and that neither the management agent configuration nor the protocol entity implementation is altered.\n\nThe alarm indicates that the switch has restarted and is now reinitializing itself. This is not necessarily an error condition but might be caused by maintenance operations such as powering up a new switch or intentional restarting of a switch after a software or configuration update. In these cases, this alarm can be safely ignored.\nHowever, a spontaneous restart should be considered as an indication of a serious problem even though the system with its redundant Ethernet infrastructure will tolerate it.\n\nClear the alarm with an alarm management application after correcting the\nfault as presented in Instructions.		

Table 41-228 SWITCH_RESTARTED (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm can be safely ignored if restarting of the switch was intentional, for example, as a part of a system reboot. In case of a random, spontaneous restart it can be very difficult to determine the cause of the abnormal behavior. \nRule out possible operation errors such as accidental issuing of a restart command or physical removal and reinsertion of the switch. Note that depending on your hardware, there may be other functions - like fibre channel (FC) switches - integrated in the same blade with the Ethernet switch. In these cases, operations done with the FC switch may, as a side effect, cause restarting of the Ethernet switch.\nTry to rule out possible power feed problems. For example:\n1. If the chassis has a management unit - such as Advanced Management Module in IBM BladeCenter environments or Onboard Administrator in HP BladeSystem environments - log in to the active management unit and check the logs and power status of the chassis.\n2. Watch for other alarms indicating a failing power stage.\n3. Watch for alarms indicating that other units are restarting in the same chassis at the same time.\n4. Rule out the possibility of someone accidentally turning the power off of the whole chassis.\n5. Rule out the possibility of a power cut in the general power supply.\nConnect to the restarted switch and try to find any indication of problems. For example:\n1. Check the switch log and look for log entries indicating hardware or software problems: for example, buffer overflows, need to restart queue engine or bad sensor readings.\n2. Check the switch statistics and look for signs of, for example, abnormally high error counter readings or buffering delays. These can be an indication of failing hardware.\n3. Check also for abnormally high load figures: problems and/or poorly configured network (for example loops) can cause major switching problems.\nMake sure that you are using a correct/recommended switch software version. If there is a version recommended by the platform, use it.\nIf the cause of the spontaneous restart cannot be found, and the switch seems to be operating correctly, ignore the alarm. However, if the problem persists and/or reappears, replace the switch blade.		

Table 41-229 SW_SET_ACTIVATION_FAILED

Alarm	Attributes	Applicable major release
Name: SW_SET_ACTIVATION_FAILED (11787) Type: environmentalAlarm Package: racloms.SW_SET_ACTIVATION_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SW SET ACTIVATION FAILED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: SW SET ACTIVATION FAILED\n\nSoftware Set activation has failed.\n\nOMS will not be restarted with the new SW Set. Old SW Set will be still active. No SW Set status (active/passive) will change.\n\nAlarm shall be cleared automatically after OMS restart or when new request for activation was received or manually by the Operator.		
Remedial action: Operator shall check Nwi3SWAgent logs to determine what caused activation failure.		

Table 41-230 SW_SET_POSTACTIVATION_SCRIPT_EXECUTION_ERROR

Alarm	Attributes	Applicable major release
Name: SW_SET_POSTACTIVATION_SCRIPT_ EXECUTION_ERROR (11788) Type: environmentalAlarm Package: racloms.SW_SET_POSTACTIVATION_ SCRIPT_EXECUTION_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SW SET POSTACTIVATION SCRIPT EXECUTION ERROR Implicitly cleared: false Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: SW SET POSTACTIVATION SCRIPT EXECUTION ERROR\n\nError has occurred during the Postactivation Scripts execution.\n\nNewly activated Software Set may not be fully functional as postactivation commands were not performed.\n\nThe user should clear the alarm manually.		

Table 41-230 SW_SET_POSTACTIVATION_SCRIPT_EXECUTION_ERROR (continued)

Alarm	Attributes	Applicable major release
Remedial action: The user should check Nwi3SWAgent and Postactivation Scripts logs to determine\nwhat caused failure. The user should execute the remaining part of the scripts manually.		

Table 41-231 SYSTEM_CLOCK_OUT_OF_SYNC_WITH_NTP_SERVER

Alarm	Attributes	Applicable major release
Name: SYSTEM_CLOCK_OUT_OF_SYNC_WITH_ NTP_SERVER (11789) Type: equipmentAlarm Package: racloms.SYSTEM_CLOCK_OUT_OF_ SYNC_WITH_NTP_SERVER Raised on class: racloms.OMS	Severity: indeterminate Specific problem: SYSTEM CLOCK OUT-OF-SYNC WITH NTP SERVER Implicitly cleared: true Default probable cause: CLOCK_ SYNCHRONISATION_PROBLEM	Release: • LOMS16A
Description: SYSTEM CLOCK OUT-OF-SYNC WITH NTP SERVER\n\nThe local clock is not accurately synchronized with the Network Time Protocol (NTP) time sources. This alarm is raised because the time difference between local and NTP sources is longer than the configured number of seconds.\n\nWhen this alarm is raised, the system time is not in sync with the NTP server and is noticeable by the operator. The system cannot be used for distributed applications that require correctly synchronized network time (i.e. IPSEC-VPN establishment). This will make system logs unreliable. Incorrect timestamps will be done by the system leading to security vulnerabilities, wrong auditing, accounting and authentication and incorrect functioning of the network file system (NFS). An inaccurate system clock also affects the operator billing system.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Disclaimer: The instructions below use either unsupported SCLI commands,\nor commands from the unsupported full bash shell. Please carefully read\nthe disclaimer that is shown when either entering the unsupported SCLI\nvendor mode or the full bash shell. Do not use the commands in any other\ncontext. Please check from the product documentation or from your local\ntechnical support for more information.\n\n1. Execute the following SCLI command to start an external bash shell session:\n\nshell bash full\n\n2. Execute the following command to check whether /ClusterNTP is in sync with\nserver ntp:\n\nntpdc -np\n\nIn the output, there should be an asterisk mark (*) on the ntp server IP, which\nindicates that it is synching with the ntp server and the alarm has been cleared\nautomatically.\n\nIf there is a cross mark (x) on the ntp server ip, refer step 8.\n\n3. Use the "exit" command to exit the bash shell.\n\n4. Execute the following SCLI command to find the ntp server IP:\n\nshow networking-service ntp\n\n5. If the asterisk (*) is not present on the ntp server IP (in output of step\n# 2), then wait for approximately 20 minutes and check whether alarm has been\ncleared using the following SCLI command:\n\nshow alarm active filter-by specific-problem 70377\n\n6. If alarm is not cleared, use the following SCLI command to sync the system\nclock with the NTP server by restarting the /ClusterNTP.\n\nset has restart managed-object /ClusterNTP\n\n7. In case you need to sync the clock of other nodes (that is, NLN), use the\nfollowing SCLI command:\n\nset has restart managed-object /NodeNTP\n\n8. If the cross mark (x) is present on the ntp server IP (in output of step\n# 2), it means the ntpd has declared the server as falseticker. This situation\narises when configured servers (two servers configuration) are not stable (not\ngiving consistent time), it results in high "jitter" and "delay"\nvalue and it will not be syncing with that server. The ntp configuration with\ntwo servers is not recommended because when there are two servers, and both\nof them claim to be authoritative but provides different times, the ntpd will\nnot be able to decide between them. Hence it will consider both the servers\nas charlatans and mark them as falsetickers.\n\nAs a solution to this problem, use either one or three servers in the ntp configuration\nfor clock sync. \n\na. If there are two existing servers and it is decided to have three servers,\nuse the below SCLI command to configure the additional server:\n\nset networking-service ntp add-forwarder <server ip-address>\n\nb. If there are two existing servers and it is decided to have one server, use\nthe below command to remove the extra server:\n\nset networking-service ntp delete-forwarder <server ip-address>		

Table 41-232 TAKING_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED

Alarm	Attributes	Applicable major release
Name: TAKING_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED (11790) Type: processingErrorAlarm Package: racloms.TAKING_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: TAKING CHECKPOINT OF IN-MEMORY DATABASE FAILED Implicitly cleared: true Default probable cause: UNDERLYING_RESOURCE_UNAVAILABLE	Release: • LOMS16A
Description: TAKING CHECKPOINT OF IN-MEMORY DATABASE FAILED\n\nAn attempt to take a checkpoint of an in-memory database has been failed.\n\nThe new checkpoint file is not written to the disk. The transaction log files are not purged. The accumulation of log files may cause the disk to run out of space and thus to total unavailability of the database instance. Moreover, the accumulation may result in a lengthy recovery operation in the case of a data store crash.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Refer to /var/opt/TimesTen/sys.odbc.ini of the node running the database instance in question. Try to determine the time of the next checkpoint from CkptFrequency and the CkptLogVolume attributes. \n2. Use the parameter management application to check when the checkpoint status is next checked. Attribute fsdbCheckpointStatusCheckInterval of the database defines the checking interval.\n3. Wait until the next checkpoint takes place and the check is completed; use the alarm management application to check whether the alarm stays in active alarms list.\n4. If the next checkpoint also fails, check the reason for the failure and continue according to the respective procedures.\nIf the reason for the alarm is "OngoingBackupOrCheckpoint"\n1. A backup or some other checkpoint operation for the data storage is in progress. The completion time for the backup depends on the size of the database: in some cases it may take a couple of minutes. Wait until the ongoing backup or checkpoint operation is completed.\n2. Wait until the next scheduled checkpoint takes place and the check is completed; use the alarm management application to check whether the alarm stays in the active alarms list.\n3. Wait until the next checkpoint takes place and the check is completed; use the alarm management application to check whether the alarm stays in active alarms list.\n4. If also next checkpoint fails contact your local Nokia representative.\nIf the reason for the alarm is "TimeOut" or "Failure"\n1. Collect following information:\n- contents of current syslog (/var/log/master-syslog)\n- output of command 'ttStatus -v'\nand contact your local Nokia representative and provide them with this information.		

Table 41-233 TAKING_SCHEDULED_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED

Alarm	Attributes	Applicable major release
Name: TAKING_SCHEDULED_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED (11791) Type: processingErrorAlarm Package: racloms.TAKING_SCHEDULED_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: TAKING SCHEDULED CHECKPOINT OF IN-MEMORY DATABASE FAILED Implicitly cleared: false Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: TAKING SCHEDULED CHECKPOINT OF IN-MEMORY DATABASE FAILED\n\nTaking scheduled checkpoint of in-memory database failed.\n\nThe new checkpoint file is not written to the disc. The transaction log files are not purged. The accumulation of log files may cause the disk to run out of space. Moreover, the accumulation may result in a lengthy recovery operation in the case of a data store crash.\n\nClear the alarm with alarm management application after correcting the fault as presented in INSTRUCTIONS.		

Table 41-233 TAKING_SCHEDULED_CHECKPOINT_OF_IN_MEMORY_DATABASE_FAILED (continued)

Alarm	Attributes	Applicable major release
Remedial action: Note: In these instructions, TimesTen is referring to the concept in-memory database.\n\n1. Determine the node from the Identifying Additional Info field of the alarm, in other words, the node where the database in question resides.\n\n2. Log into the database node.\n\n3. In the node where the alarm was raised, determine the directory of the checkpoint files (.ds0 and .ds1) for the database in question with the following command:\n\n ttStatus\n\nSee data management documentation for more instructions about the ttStatus command.\n\n4. Check the timestamps of the checkpoint files of the database.\n\nIf the timestamp of one of the checkpoints is later than the time of the alarm, the next checkpoint has been successful and the alarm can be cleared.\n\n5. If the alarm still has the latest timestamp compared to the checkpoint files of the database, gather the following information:\n\n a. Copy the original master-syslog to the temporary directory.\n cp /var/log/master-syslog /tmp/<filenameA>.<extension>\n Select filenameA and extension, for example, <alarm_number>_syslog.log.\n\n b. Move to the tmp directory.\n cd /tmp\n\n c. In the node where the alarm was raised, determine the TimesTen status.\n ttStatus -v > /tmp/<filenameB>.txt\n Select filenameB, for example, <alarm number>_ttstatus.log. The requirement is that filenameB differs from filenameA.\n\n d. Compress the files with the tar command. \n tar -cf <tarname>.tar <filenameA>.<extension> <filenameB>.txt\n Select tarname, for example, <alarm number>.tar.\n\nNote that the tar command does not delete the original files. When the files are not needed anymore, they can be deleted. \n\n e. Contact your Nokia representative with the information gathered.		

Table 41-234 THRESHOLD_MONITORING_LIMIT_EXCEEDED

Alarm	Attributes	Applicable major release
Name: THRESHOLD_MONITORING_LIMIT_ EXCEEDED (11792) Type: qualityOfServiceAlarm Package: racloms.THRESHOLD_MONITORING_ LIMIT_EXCEEDED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: THRESHOLD MONITORING LIMIT EXCEEDED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: THRESHOLD MONITORING LIMIT EXCEEDED\n\nThreshold monitoring makes it easier to detect faults, identify bottlenecks and optimize the network. Using Element Manager GUI, appropriate performance thresholds are determined for each important variable, and exceeding these thresholds indicates a problem worth of attention. These variables can be either single counters or Key Performance Indicators (KPIs), which can be a combination of several counters.\n \nWhen performance data is gathered on variables of interest from the measured objects in the network, their values are compared against any active threshold limits. When a performance threshold is exceeded, an alarm is generated and sent to the network management system. In addition to this, a threshold event log is saved in the network element for further study of the events which have occurred in that NE during a certain period of time.\n \nWhen this alarm has been triggered, it means that a threshold monitoring rule has been evaluated as true by OMS. The object of this alarm is always OMS, even if the threshold rule had been targeted to some other measured object. The real object of the threshold alarm and more information on the event can be seen with the NE Threshold Management application.\n\nThe effect of this alarm is dependent on what is the operator defined threshold rule that triggered the alarm setting.\n\nDo not clear the alarm. This alarm is cancelled automatically by the system after 15 seconds.		
Remedial action: Threshold alarm does not necessarily mean that there are problems in the network element, because thresholds can be freely set by the operator, and some rules may have been set incorrectly.\n \nTo get further information on the reason of the threshold alarm:\n \n- Connect to the network element with Element Manager.\n- Open the NE Threshold Management application.\n- Select "Show Threshold Log" from the View menu and check the threshold log.\n \nWhen the target object and other information of the alarm have been checked from the log, you can obtain more information from the performance counters of measurements and, if necessary, take appropriate action to correct the problem. The counters can be browsed either by using Element Manager applications (NE Measurement Explorer or RNW Measurement Presentation) or by using NetAct reporting tools.		

Table 41-235 THRESHOLD_VALUE_EXCEEDED_IN_ETHERNET_DEVICE

Alarm	Attributes	Applicable major release
Name: THRESHOLD_VALUE_EXCEEDED_IN_ETHERNET_DEVICE (11793) Type: qualityOfServiceAlarm Package: racloms.THRESHOLD_VALUE_EXCEEDED_IN_ETHERNET_DEVICE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: THRESHOLD VALUE EXCEEDED IN ETHERNET DEVICE Implicitly cleared: false Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: THRESHOLD VALUE EXCEEDED IN ETHERNET DEVICE\n\nThe Utilization Flag indicates that the utilization value has been exceeded from the port/interface. \n\nThe Remote Monitoring system periodically takes statistical samples from the various Ethernet variables, the oversize/undersize packet count, number of broadcast packets, Octets of data etc. and compares these to thresholds that have been configured. The alarm table stores configuration entries that each defines a variable, polling period, and threshold parameters. If a sample is found to cross the threshold values, an event is generated. This mechanism generates one event as a threshold is crossed in the appropriate direction. No more events are generated for that threshold until the opposite threshold is crossed. This object can be used as a reasonable estimate of Ethernet utilization. The result equation is the value Utilization that is the percent utilization of the Ethernet segment on a scale of 0 to 100 percent.\n\nThe Rising RMON Alarm trap is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. \n\nThe Falling RMON Alarm trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.\n\nThese traps indicate a change in the threshold of one or more of the Ethernet counters. If the traffic through some port/interface is too heavy, it can prevent some important service or server functionality behind that port/interface.\n\nClear the alarm with the Alarm Browser after correcting the fault as presented in INSTRUCTIONS.		
Remedial action: Check the LAN configuration. Check the interface(s) that have sent Rising/Falling Alarm. Check also the network topology and the reason for the increased traffic in the interface.		

Table 41-236 TRACE_CONNECTION_TO_NE_IS_LOST

Alarm	Attributes	Applicable major release
Name: TRACE_CONNECTION_TO_NE_IS_LOST (11794) Type: communicationsAlarm Package: racloms.TRACE_CONNECTION_TO_NE_IS_LOST Raised on class: racloms.OMS	Severity: indeterminate Specific problem: TRACE CONNECTION TO NE IS LOST Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: TRACE CONNECTION TO NE IS LOST\n\nTrace connection to NE is lost. This might happen when synchronization with NE to OMS is lost, connection is interrupted or there is overload situation.\n\n-\n\nAlarm is cancelled automatically after time to live for the alarm has elapsed.		
Remedial action: -		

Table 41-237 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • LOMS16A
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 41-238 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • LOMS16A
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		

Table 41-238 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 41-239 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw.TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • LOMS16A
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 41-240 TROUBLESHOOTING_DATA_CREATION_OR_UPLOAD_FAILED

Alarm	Attributes	Applicable major release
Name: TROUBLESHOOTING_DATA_CREATION_OR_UPLOAD_FAILED (11795) Type: communicationsAlarm Package: racloms.TROUBLESHOOTING_DATA_CREATION_OR_UPLOAD_FAILED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: TROUBLESHOOTING DATA CREATION OR UPLOAD FAILED Implicitly cleared: true Default probable cause: TRANSMISSION_FAILURE	Release: • LOMS16A
Description: TROUBLESHOOTING DATA CREATION OR UPLOAD FAILED\n\nThere was a problem in requesting troubleshooting data collection or during troubleshooting data upload.\n\nTroubleshooting data is not available.\n\nDo not clear the alarm. System clears the alarm automatically.		
Remedial action: Depending on the failure reason the operation of troubleshooting data request may be renewed. In particular, if there was some problem during file transfer or operation timeout happened.		

Table 41-241 TROUBLESHOOTING_DATA_RECEIVED

Alarm	Attributes	Applicable major release
Name: TROUBLESHOOTING_DATA_RECEIVED (11796) Type: environmentalAlarm Package: racloms.TROUBLESHOOTING_DATA_RECEIVED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: TROUBLESHOOTING DATA RECEIVED Implicitly cleared: true Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: TROUBLESHOOTING DATA RECEIVED\n\nTroubleshooting file is received from the NE.\n\nThe file is available in OMS disk.\n\nDo not clear the alarm. System will clear the alarm automatically.		
Remedial action: Troubleshooting file uploaded by NE is available in OMS disk from /var/opt/OMSftproot/NE/TroubleshootingData.\nThe troubleshooting file is kept in OMS disk for a configurable amount of time (the default value, configured by the dwNELogDaysSpan parameter, is 10 days).\n\nHowever, this troubleshooting file is automatically deleted in OMS in the following cases:\n\n1) If the available storage space in OMS is getting full, also younger files - that is files stored for at least 2 hours (or equivalently, 120 minutes, as per the default value of the related configuration parameter - dwBTSLogObsolescenceTimeMins) - shall be deleted.\n\n2) When the troubleshooting data file is already uploaded to NetAct in the following situations:\n\n a) For Troubleshooting Data Collection and Upload requested by NetAct User, OMS notifies NetAct about availability of file/s and NetAct uploads the file/s from OMS.\n\n b) For NE triggered troubleshooting log collection, OMS notifies NetAct about availability of the file and NetAct uploads the file from OMS.\n\n \nNote 1: When the troubleshooting data file is still available in OMS disk, it can be viewed in OMS Web UI and can also be downloaded to user's local disk.\nNote 2: When the troubleshooting data file is already uploaded to NetAct:\n\n - In OSS5.x system troubleshooting files can be found from /var/opt/nokia/oss/global/ltemei/lte_ne_symptom_file in CS-2 server.\n\n - In NetAct8 system troubleshooting files can be found from /var/opt/oss/global/nwi3/ne_symptom_files.		

Table 41-242 UNEXPECTED_CONNECTIONS_TO_IN_MEMORY_DATABASE_HAVING_STANDBY_ROLE

Alarm	Attributes	Applicable major release
Name: UNEXPECTED_CONNECTIONS_TO_IN_MEMORY_DATABASE_HAVING_STANDBY_ROLE (11797) Type: processingErrorAlarm Package: racloms.UNEXPECTED_CONNECTIONS_TO_IN_MEMORY_DATABASE_HAVING_STANDBY_ROLE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNEXPECTED CONNECTIONS TO IN-MEMORY DATABASE HAVING STANDBY ROLE Implicitly cleared: true Default probable cause: SOFTWARE_ERROR	Release: • LOMS16A
Description: UNEXPECTED CONNECTIONS TO IN-MEMORY DATABASE HAVING STANDBY ROLE\n\nOne or more connections exist to an in-memory database that has a standby role.\n\nThe Level of the database high availability is slightly reduced. In a case of serious replication problems the in-memory database watchdog process is not able to attempt to fix the problem by duplicating the database. In this case the database is, in effect, a standalone database and a separate alarm (70171) is raised.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Wait for a while and check whether the alarm persists. If the alarm is not cleared automatically within minute, check the processes that are connected to the database as follows:\n1. Connect to the node having the database instance as root.\n2. Check identifiers of processes that are connected to the database by running the ttStatus command. The command lists connections to each database in that node. Concentrate on the database of this alarm and look at connections of the type Process or Server.\n3. For each type of Process connection look at the process identifier (pid) of the connected process and run the command\nps p <pid>\n(<pid> is the process identifier) in same node where the database is located in order to see the connected process.\n4. For each type of Server connection look at the client information below and pick process identifier (pid) and node name. Run the following command\nssh <node> "ps p <pid>"\n(<node> is the node and <pid> process identifier you picked from the client information) to see the connected process.\nContact your local NSN representative and provide the information you obtained from the ttStatus and ps commands.		

Table 41-243 UNEXPECTED_PERSISTENT_STATUS_DATA_VALUES_FOR_IN_MEMORY_DATABASE

Alarm	Attributes	Applicable major release
Name: UNEXPECTED_PERSISTENT_STATUS_DATA_VALUES_FOR_IN_MEMORY_DATABASE (11798) Type: processingErrorAlarm Package: racloms.UNEXPECTED_PERSISTENT_STATUS_DATA_VALUES_FOR_IN_MEMORY_DATABASE Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNEXPECTED PERSISTENT STATUS DATA VALUES FOR IN-MEMORY DATABASE Implicitly cleared: false Default probable cause: APPLICATION_SUBSYSTEM_FAILURE	Release: • LOMS16A
Description: UNEXPECTED PERSISTENT STATUS DATA VALUES FOR IN-MEMORY DATABASE\n\nPersistent status data values for a replicated pair of in-memory databases have become corrupted (inconsistent combination of values or erroneous single value).\n\nThe database high availability (HA) service for the in-memory database cannot determine which of the databases should accept the active role. The watchdog process cannot enable the database and application does not connect to any of the database instances. Manual recovery is required.\n\nClear the alarm with alarm management application after correcting the fault as explained in INSTRUCTIONS.		
Remedial action: 1. Check the persistent status info in application additional info for types or invalid combinations. The valid combinations are:\n("","","","")\n("active","sync","","")\n("active","oosync","","")\n("active","oosync", "active","sync")\n("active","duplicate","","")\n("active","duplicate","active","sync")\n("standby", "sync","active","sync")\n("standby","sync","active","oosync")\n("standby","sync","active", "duplicate")\n("standby","oosync","active","sync")\n("standby","oosync","active","oosync")\n("standby","oosync","active,"duplicate")\nplus all the combinations made from above combinations by swapping persistent role and peer persistent role, and persistent status and peer persistent status.\n\n2. If a typo is found and it is known that the values have been updated manually, correct the value with the fshascli command as illustrated in the following example:\nfshascli -S Role="active fsdbHostName=TA-A,fsdbName=DB_TestTT, fsFragmentId=DB,fsClusterId=ClusterRoot\n\n3. If an invalid value combination is found, try to validate it if one of the database instances is able to play an active role. Then, use the fshascli-command to set the correct combination. For example, if an instance of node TA-A gets the active role an and instance of TA-B the standby role, use the following commands to correct the status:\nfshascli -S Role=standby fsdbHostName=TA-B,fsdbName=DB_TestTT,fsFragmentId=DB,fsClusterId=ClusterRoot\nfshascli -S State=oosync fsdbHostName=TA-B,fsdbName=DB_TestTT,fsFragmentId=DB,fsClusterId=ClusterRoot\nfshascli -S Role=active fsdbHostName=TA-A, fsdbName=DB_TestTT,fsFragmentId=DB,fsClusterId=ClusterRoot\nfshascli -S State=oosync fsdbHostName=TA-A,fsdbName=DB_TestTT,fsFragmentId=DB,fsClusterId=ClusterRoot\nThe in-memory database watchdog process checks periodically the persistent status data and will enable the TA-A instance after a while."		

Table 41-244 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • LOMS16A
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 41-245 UNKNOWN_SNMP_TRAP

Alarm	Attributes	Applicable major release
Name: UNKNOWN_SNMP_TRAP (11799) Type: processingErrorAlarm Package: racloms.UNKNOWN_SNMP_TRAP Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNKNOWN SNMP TRAP Implicitly cleared: false Default probable cause: CORRUPT_DATA_M3100	Release: • LOMS16A
Description: UNKNOWN SNMP TRAP\n\nThe SNMP Mediator has received an SNMP trap that it is unaware of. The trap is unknown to the SNMP Mediator, if\n1) the IP address of the SNMP agent that sends the trap is missing from the SNMP Mediator's configuration, or\n2) the OID (object identifier) of the trap is unknown to the SNMP Mediator.\n\n1) Unknown traps may contain information that could be useful. \n2) Unnecessary traps waste network capacity.\n\nClear the alarm with the fault management application after correcting the fault.		
Remedial action: 1. Using the parameter management application, check that the IP address of the SNMP agent is stored in the SNMP Mediator's configuration. An entry of the following format should be found:\nfssnmpNEId="<agent IP or hostname>,\nfssnmpAttribute-Type=NEattrs, \nfssnmpMediatorName=1,\nfsFragmentId=SNMP,\nfsClusterId=ClusterRoot\n\n2. If the trap is unnecessary, \n check whether there is a way to disable the sending of the trap in the SNMP agent or \n use filtering in the SNMP Mediator. The SNMP Mediator may be configured to filter out traps by adding an entry of the following format:\nfssnmpV2TrapId=<trap OID>\ nfssnmpAttributeType=V2traps, \nfssnmpMediatorName=1,\nfsFragmentId=SNMP,\nfsClusterId=ClusterRoot\nIf the above entry without attributes exists in the configuration, the SNMP Mediator will ignore the trap and no alarm is raised. Additionally, filtering attributes fssnmpAcceptFrom or fssnmpDiscardFrom may be used to define the IP addresses from where the trap should be accepted or ignored. Attribute fssnmpFilterCondition may be used for filtering away traps based on variables within the trap itself. See RFC 2254 for information about the filter syntax ("approx", "extensible" and "escaping mechanism" are not supported).\n3. If the trap contains important information, the implementation of the SNMP Mediator should be updated. The rules that define what the SNMP Mediator does when it receives traps are part of the implementation. Fill in a problem report and send it to your local Nokia representative."		

Table 41-246 UNKNOWN_SPECIFIC_PROBLEM

Alarm	Attributes	Applicable major release
Name: UNKNOWN_SPECIFIC_PROBLEM (11800) Type: processingErrorAlarm Package: racloms.UNKNOWN_SPECIFIC_PROBLEM Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNKNOWN SPECIFIC PROBLEM Implicitly cleared: true Default probable cause: CONFIGURATION_OR_ CUSTOMIZING_ERROR	Release: • LOMS16A
Description: UNKNOWN SPECIFIC PROBLEM\n\nThis alarm indicates detection of an alarm notification for a specific problem (alarm number) that is unknown to the alarm system (the corresponding alarm type isn't defined in the reference data).\n\nThe unknown specific problem can be the result of either using a dynamic alarm type (a type that isn't inherently predefined and correspondingly not ported to the alarm system) or a mistake due to a missing import of the existing alarm definition in the alarm system.\n\nThe alarm system creates a new type of alarm on the fly, using data from the alarm notification to set the alarm type parameters. This alarm type is stored persistently in the alarm system database reference data and applied to subsequent new alarm notifications that contain the specific problem in question, which results in no longer raising alarm 70280 in a case of the recently registered specific problem.\n\nThe alarm system clears the alarm automatically after its time to live\nhas expired.		

Table 41-246 UNKNOWN_SPECIFIC_PROBLEM (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm either announces the use of a dynamic alarm type in alarm notification or indicates an undefined alarm in the alarm system (the exact reason can be identified by checking the list of known alarms in the customer documentation). In the latter case contact your Nokia representative to upgrade the system with the missing alarm definition.\n\nThe alarm system creates a new alarm type using the following values for its parameters:\n\nA. Static parameters:\n\n1. Alarm text - the value of a special field in the alarm notification; if the field isn't defined then the text takes the following form: "ALARM NNN" where NNN is the specific problem in question.\n2. Probable cause - 0 (INDETERMINATE).\n3. Event type - Environmental.\n4. Specific problem - the specific problem in question.\n5. Clearing info - automatic clearing.\n\nB. Dynamic parameters:\n\n6. Default severity - the perceived severity of the alarm notification; if it isn't set then the INDETERMINATE value is used.\n7. Autoacknowledgment - yes, if the fsParameterId= "fsAutoAckedDAT,\nfsAlarmProcessorConfigurationId=Default, fsAlarmProcessorId=AlarmProcessor1,\nfsFragmentId= AlarmProcessors, fsFragmentId=AlarmMgmt, fsClusterId=ClusterRootdefined attribute in the alarm system LDAP configuration is set to "true"; otherwise - no.\n8. Switch over update - no.\n9. Clearing delay - 0.\n10. Informing delay - 0.\n11. Time to live - 0.\n12. Operation Instructions - "Not defined".\n \nIf required, the static parameters can be changed with an alarm management application."		

Table 41-247 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • LOMS16A
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 41-248 UNRECOMMENDED_CONFIGURATION_FORCED_BY_OPERATOR

Alarm	Attributes	Applicable major release
Name: UNRECOMMENDED_CONFIGURATION_ FORCED_BY_OPERATOR (11801) Type: equipmentAlarm Package: racloms.UNRECOMMENDED_ CONFIGURATION_FORCED_BY_OPERATOR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: UNRECOMMENDED CONFIGURATION FORCED BY OPERATOR Implicitly cleared: true Default probable cause: EQUIPMENT_ MALFUNCTION	Release: • LOMS16A

Table 41-248 UNRECOMMENDED_CONFIGURATION_FORCED_BY_OPERATOR (continued)

Alarm	Attributes	Applicable major release
Description: UNRECOMMENDED CONFIGURATION FORCED BY OPERATOR\n\nServices that are critical to the system operation are provided in the CLA-0 and CLA-1 nodes using an active-standby redundancy model. The most important service is called Directory. \nOne of the following has happened: \n\na) An operator has, by issuing a switchover or lock command, forced the Directory service to run in the same node as the Cluster Management Functionality (CMF). \n\nb) An operator has locked the current standby FSDirectoryServer recovery unit. The Directory and Cluster Management Functionality services are, however, not running in the same node.\n\nc) An operator has, by issuing CFM yield or CMF disable command, forced the master CMF to run in the same node with Directory service.\n\nd) An operator has disabled both CMF services using CMF disable command and then started CMF in the same node with Directory service by issuing CMF enable command.\n\nThe system attempts to keep the services on separate nodes. If a failure or an operator action forces the services to the same node the system automatically tries to move CMF service to another node after some time. The automatic service separation however will not work if one of the CMF services is disabled or the CMF service was forced to run in the same node with Directory service by issuing a CMF yield command.\n\nThe situation has no immediate impact to system operation. The system provides services normally as long as the currently operational CLA node(s) and their services remain functional. \nAn operator can choose to set this configuration if, for example, one CLA node needs maintenance. \nIf the critical system services are currently running in the same node, a node failure causes their services to be down for some time. Especially the Directory service switchover can last considerably longer than usual. Directory service downtime has often immediate impact on the services provided by the network element, because the shared system disk is unavailable.\nIf the critical services of the system are running on separate CLA nodes, but the FSDirectoryServer recovery unit is locked in one CLA node, failure of the node that provides the Directory service causes the Directory service to be down for a few minutes (until the node has successfully rebooted) or permanently (if the node fails to start).\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: Find out why the Directory service has been forced to run in the same node as the Cluster Management Functionality or why an FSDirectoryServer recovery unit has been locked.\nIf the situation was not intentional, the system can be restored to a safer state by performing the following steps: \n1. Log into the system as root user. \n2. Check the status of the FSDirectoryServer recovery units using the fshascli command: \n$ fshascli --state "/*/FSDirectoryServer"\n/CLA-0/FSDirectoryServer:\nadministrative(UNLOCKED)\noperational(ENABLED)\nusage(ACTIVE)\nprocedural()\navailability()\nunknown(FALSE)\nalarm()\nrole(ACTIVE)\n\n/CLA-1/FSDirectoryServer:\nadministrative(LOCKED)\noperational(ENABLED)\nusage(IDLE)\nprocedural(NOTINITIALIZED)\navailability(OFFDUTY)\nunknown(FALSE)\nalarm()\nrole(COLDSTANDBY)\n\n3. If one of the recovery units is LOCKED, unlock it using the fshascli command. For example: \n$ fshascli --unlock /CLA-1/FSDirectoryServer\n/CLA-1/FSDirectoryServer is unlocked successfully.\n\n4. Once both recovery units are unlocked, you need to check if the Directory service is running in the same CLA node as the Cluster Management Functionality. Use the fshascli command to check which one of CLA node is providing the service. \n$ fshascli --state "/*/FSDirectoryServer"\n/CLA-0/FSDirectoryServer:\nadministrative(UNLOCKED)\noperational(ENABLED)\nusage(ACTIVE)\nprocedural()\navailability()\nunknown(FALSE)\nalarm()\nrole(ACTIVE)\n\n/CLA-1/FSDirectoryServer:\nadministrative(UNLOCKED)\noperational(ENABLED)\nusage(IDLE)\nprocedural(NOTINITIALIZED)\navailability()\nunknown(FALSE)\nalarm()\nrole(COLDSTANDBY)\n\nThe recovery unit that has the ACTIVE role is providing the service. Note that the operational recovery unit must also have operational state ENABLED, usage state ACTIVE and the procedural status value must be empty. \n\n5. Use the fscmfcli command to check which node is providing the Cluster Management Functionality. Note that with the --status option, the fscmfcli expects the node managed object name of an operational CLA node. If both CLA nodes are operational, it does not matter which one is specified. For example, \n$ fscmfcli --status /CLA-0\nCLA-0: CMF-SERVING priority: 5\nCLA-1: CMF-DISABLED priority: 6 \n\n6. If the services are provided by different nodes, no further actions are required. \nIn the example situation the services are both provided by the CLA-0 node. The situation can be solved by forcing either Directory or CMF service to another node. Usually a CMF switchover is recommended as the Directory service switchover takes more time and applications using the services provided by the Directory will be un-operational during the switchover. In this case the backup CMF is disabled which will prevent the CMF switchover. The backup CMF needs to be enabled first;\n$ fscmfcli --enable /CLA-1\nCluster management functionality enabled on host CLA-1\n$ fscmfcli -s /CLA-0\nCLA-0: CMF-SERVING priority: 5\nCLA-1: CMF-BACKUP priority: 6\n\n7. After both of the CMF services are enabled the CMF service can be switched over to backup node:\n$ fscmfcli --yield /CLA-0\nHost CLA-0 is giving up active role.\n$ fscmfcli -s /CLA-0\nCLA-0: CMF-BACKUP priority: 5\nCLA-1: CMF-SERVING priority: 6\n\n8. If you choose to execute a Directory service switchover, enter the following fshascli switchover command: \n$ fshascli --switchover --nowarning --force /Directory\n/Directory switchover done successfully\n\nNote that if your terminal connection to the cluster was established to the Directory service IP address, your terminal connection is closed and you must log in again.		

Table 41-249 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • LOMS16A
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 41-250 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • LOMS16A
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 41-251 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • LOMS16A
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 41-252 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • LOMS16A
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 41-253 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • LOMS16A
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 41-254 VOLTAGE_OUT_OF_LIMIT

Alarm	Attributes	Applicable major release
Name: VOLTAGE_OUT_OF_LIMIT (11802) Type: equipmentAlarm Package: racloms.VOLTAGE_OUT_OF_LIMIT Raised on class: racloms.OMS	Severity: indeterminate Specific problem: VOLTAGE OUT OF LIMIT Implicitly cleared: true Default probable cause: POWER_SUPPLY_FAILURE	Release: • LOMS16A
Description: VOLTAGE OUT OF LIMIT\n\nThe unit's voltage has exceeded the programmed threshold value(high or low values).\n\nThe unit may behave erratically.\n\nThe system clears the alarm automatically when the fault has been corrected.		
Remedial action: 1. Check that the input voltage of the power feed in the cabinet is correct.\n\n2. Check that the affected unit is healthy, and is plugged-in properly.\n\n3. Restart the unit, if necessary.\n\n4. Replace the unit, if necessary.\n\n5. If the problem exists even after following the instructions, please contact your local customer support.		

Table 41-255 WARNINGS_REPORTED_FOR_MSU_AUTOMATIC_POSTCONFIGURATION

Alarm	Attributes	Applicable major release
Name: WARNINGS_REPORTED_FOR_MSU_AUTOMATIC_POSTCONFIGURATION (11803) Type: environmentalAlarm Package: racloms.WARNINGS_REPORTED_FOR_MSU_AUTOMATIC_POSTCONFIGURATION Raised on class: racloms.OMS	Severity: indeterminate Specific problem: WARNINGS REPORTED FOR MSU AUTOMATIC POSTCONFIGURATION Implicitly cleared: false Default probable cause: INDETERMINATE	Release: • LOMS16A
Description: WARNINGS REPORTED FOR MSU AUTOMATIC POSTCONFIGURATION\n\nThe OMS has detected WARNINGS in the log files. The warnings were reported in the last phase of a major software upgrade (MSU) procedure. The found warnings did not trigger a fallback to the previous OMS release. The OMS is working properly, but it is possible that the user data was not migrated completely.\n\nThe alarm is raised if OMS encounters warnings during checking of automatic postconfiguration logs.\n\nClear the alarm with alarm management application once the reported warnings have been investigated as presented in the Instructions.		
Remedial action: Operator should inspect WARNING entries in listed log files. In case of lack of knowledge about warnings meaning, listed log files have to be gathered by Operator into package and sent to troubleshooting team.		

Table 41-256 WCEL_THRESHOLD_MONITORING_LIMIT_EXCEEDED

Alarm	Attributes	Applicable major release
Name: WCEL_THRESHOLD_MONITORING_LIMIT_EXCEEDED (11804) Type: qualityOfServiceAlarm Package: racloms.WCEL_THRESHOLD_MONITORING_LIMIT_EXCEEDED Raised on class: racloms.OMS	Severity: indeterminate Specific problem: WCEL THRESHOLD MONITORING LIMIT EXCEEDED Implicitly cleared: true Default probable cause: THRESHOLD_CROSSED	Release: • LOMS16A
Description: WCEL THRESHOLD MONITORING LIMIT EXCEEDED\n\nWhen this alarm has been triggered, it means that a threshold monitoring rule has been evaluated as true by OMS for some WCDMA cell object in the Cell Resource measurement. More information on the event can be seen with the NE Threshold Management application in OMS Element Manager.\n\nThreshold monitoring makes it easier to detect faults, identify bottlenecks and optimize the network. Using OMS Element Manager GUI, appropriate performance thresholds are determined for each important variable, and exceeding these thresholds indicates a problem worth of attention. These variables can be either single counters or Key Performance Indicators (KPIs), which can be a combination of several counters.\n\nWhen performance data is gathered on variables of interest from the measured objects in the network, their values are compared against any active threshold limits. When a performance threshold is exceeded, an alarm is generated and sent to the network management system. In addition to this, a threshold event log is saved in the network element for further study of the events which have occurred in that NE during a certain period of time.\n\n-\n\nDo not clear the alarm. This alarm has a lifetime of 65 minutes.		
Remedial action: Threshold alarm does not necessarily mean that there are problems in the network element, because thresholds can be freely set by the operator, and some rules may have been set incorrectly.\n\nTo get further information on the reason of the threshold alarm:\n\n- Connect to the network element with Element Manager.\n\n- Open the NE Threshold Management application.\n\n- Select "Show Threshold Log" from the View menu and check the threshold log.\n\nWhen the target object and other information of the alarm have been checked from the log, you can obtain more information from the performance counters of measurements and, if necessary, take appropriate action to correct the problem. The counters can be browsed with RNW Measurement Presentation application or by using NetAct reporting tools.		

Table 41-257 WEBSPHERE_INTERNAL_ERROR

Alarm	Attributes	Applicable major release
Name: WEBSPHERE_INTERNAL_ERROR (11805) Type: processingErrorAlarm Package: racloms.WEBSPHERE_INTERNAL_ERROR Raised on class: racloms.OMS	Severity: indeterminate Specific problem: WEBSPHERE INTERNAL ERROR Implicitly cleared: true Default probable cause: SOFTWARE_PROGRAM_ERROR	Release: • LOMS16A
Description: WEBSPHERE INTERNAL ERROR\n\nWebSphere internal error is raised if there are new exceptions in the WebSphere log files. The exception can be located in the application Server SystemOut.log or under the WebSphere ffdc logs directory.\n\nThe raised Alarm is an indication of a problem that can cause the applications running inside WebSphere not to run correctly. The problem can also cause that the FlexiServer Element Manager is not able to contact the Application Server or the application deployed to WebSphere.\n\nClear the alarm with Alarm Browser after correcting the fault as presented in INSTRUCTIONS.		
Remedial action: If this alarm is raised, the operator has to make an immediate collection of the logs of WebSphere using its collector tool. The collector tool is located under the profile path bin directory </var/mnt/local/<partion_name>/profiles/<profile_name>/bin/collector.sh>. \nAs a result of using the collector tool, a new file will be created to the system "<node>-<cell_name>-<node_name>-<server_name>-WASenv.jar". This file contains all the logs from WebSphere. This file is valuable for error detection and fixing the problems. The file will be created to the same directory from which it is executed.		

Table 41-258 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • LOMS16A
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

42 OpenFlow

42.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 42-1 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • N/A
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 42-2 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 42-3 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • N/A
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 42-4 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 42-5 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 42-5 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 42-6 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • N/A
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 42-7 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • N/A
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 42-8 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 42-9 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 42-10 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 42-10 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 42-11 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • N/A
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 42-12 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • N/A
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 42-13 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 42-14 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 42-15 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • N/A
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 42-16 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 42-17 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • N/A
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 42-18 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • N/A
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 42-19 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • N/A
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 42-20 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • N/A
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 42-21 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • N/A
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		

Table 42-21 LinkDown (equipment) (continued)

Alarm	Attributes	Applicable major release
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 42-22 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • N/A
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 42-23 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • N/A
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 42-24 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • N/A

Table 42-24 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 42-25 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • N/A
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 42-26 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • N/A
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 42-27 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • N/A
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 42-28 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • N/A
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 42-29 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • N/A
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 42-30 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • N/A
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 42-31 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • N/A
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 42-32 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • N/A
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 42-33 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • N/A
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

43 OS10K

43.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 43-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 43-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 43-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 43-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 43-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 43-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 43-6 AtcaFanFailure

Alarm	Attributes	Applicable major release
Name: AtcaFanFailure (1124) Type: equipmentAlarm Package: equipment.AtcaFanFailure Raised on class: equipment.Fan	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled') OR ('operationalState' EQUAL 'Down'))		
Clearing condition: (('operationalState' EQUAL 'Enabled') OR ('operationalState' EQUAL 'Up'))		
Remedial action: This alarm is raised if the fan speed falls below 500 rpm. If the alarm persists, replace the appropriate (upper or lower) fan tray.		

Table 43-7 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		

Table 43-7 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 43-8 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 43-9 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-10 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 43-11 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 43-12 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 43-13 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 43-14 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 43-15 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 43-16 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		

Table 43-16 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 43-17 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 43-18 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 43-19 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 43-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 43-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		

Table 43-21 EquipmentDegraded (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 43-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 43-23 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-24 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 43-25 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 43-26 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		

Table 43-26 EquipmentRemoved (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 43-27 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 43-28 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 43-29 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 43-30 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 43-31 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		

Table 43-31 EthernetPortNoAmLock (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 43-32 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 43-33 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 43-34 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 43-35 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 43-36 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the associated fan is not operationally Up.		

Table 43-36 FanFailure (equipment) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 43-37 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 43-38 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.3.2
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 43-39 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 43-40 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 43-41 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2

Table 43-41 IfVlanSubTypeConflict (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 43-42 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 43-43 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 43-44 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 43-45 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 43-46 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2

Table 43-46 IsisDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 43-47 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 7.3.2
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 43-48 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 43-49 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 43-50 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 43-51 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		

Table 43-51 LinkDown (equipment) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 43-52 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 43-53 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 43-54 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 43-55 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 43-56 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.3.1 • 7.3.2
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 43-57 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 43-58 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 43-59 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		

Table 43-59 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 43-60 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 43-61 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		

Table 43-61 NewSsh2ServerKeyDetected (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 43-62 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 43-63 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 43-64 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 43-65 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 43-66 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		

Table 43-66 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 43-67 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 43-68 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 43-69 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 43-70 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 43-71 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2

Table 43-71 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 43-72 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 43-73 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		

Table 43-73 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 43-74 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-75 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-76 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-77 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-78 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		

Table 43-78 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 43-79 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-80 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-81 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 43-82 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 43-83 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		

Table 43-83 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 43-84 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 43-85 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 43-86 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 7.3.1 • 7.3.2
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 43-87 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 43-88 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 43-88 RipDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 43-89 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 43-90 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 43-91 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 43-92 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 7.3.2
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 43-93 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 7.3.2
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		

Table 43-93 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 43-94 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 43-95 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 43-96 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 43-97 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.3.2
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 43-98 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 43-98 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 43-99 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 43-100 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 43-101 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 43-102 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 43-103 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		

Table 43-103 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 43-104 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 43-105 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 43-106 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 43-107 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 43-108 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 43-109 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		

Table 43-109 upgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 43-110 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 43-111 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 43-112 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 43-113 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 43-114 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2

Table 43-114 VirtualNeighborDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 43-115 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 7.1.1 • 7.2.1 • 7.3.1 • 7.3.2
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

44 OS6250

44.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 44-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 44-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 44-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 44-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 44-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 44-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 44-7 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 44-8 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 44-9 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 44-10 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 44-11 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 44-12 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 44-13 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 44-14 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 44-15 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 44-16 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 44-17 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 44-18 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 44-19 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 44-20 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 44-21 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 44-22 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 44-23 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 44-24 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment. EthernetPortConfiguredLoopback Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoop-back	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 44-25 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 44-26 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 44-27 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 44-28 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 44-29 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 44-30 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 44-31 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 44-32 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 44-33 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 44-34 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 44-35 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 44-36 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 44-37 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 44-38 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 44-39 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 44-40 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 44-41 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 44-42 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 44-43 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 44-44 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 44-45 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 44-46 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 44-47 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 44-48 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 44-49 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 44-50 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 44-51 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 44-52 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 44-53 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 44-54 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 44-55 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 44-56 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 44-57 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 44-58 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.6.5 • 6.7.1
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 44-59 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 44-60 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 44-61 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 44-62 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw.PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 44-63 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 44-64 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 44-65 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 44-66 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-67 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-68 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-69 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-70 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 44-71 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-72 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-73 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 44-74 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 44-75 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 44-76 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 44-77 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 44-78 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 44-79 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 44-80 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 44-81 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 44-82 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 44-83 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 44-84 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 44-85 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 44-86 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 44-87 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 44-88 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 44-89 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 44-90 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 44-91 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 44-92 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 44-93 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 44-93 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 44-94 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 44-95 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 44-96 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 44-97 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 44-98 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 44-99 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 44-100 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 44-101 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 44-102 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.6.1 • 6.6.2 • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

45 OS6400

45.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 45-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 45-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 45-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 45-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 45-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		

Table 45-5 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 45-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 45-7 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 45-8 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 45-9 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 45-10 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 45-11 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 45-12 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 45-12 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - no corrective action required.		

Table 45-13 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 45-14 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 45-15 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.4.3 • 6.4.4 • 6.4.5

Table 45-15 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 45-16 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 45-17 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 45-18 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 45-19 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 45-20 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 45-21 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 45-22 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 45-23 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 45-24 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 45-25 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 45-26 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		

Table 45-26 EthernetPortHighBer (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 45-27 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 45-28 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 45-29 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 45-30 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 45-31 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.4.3 • 6.4.4 • 6.4.5

Table 45-31 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 45-32 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 45-33 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 45-34 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 45-35 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 45-36 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 45-36 GaPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 45-37 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 45-38 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 45-39 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 45-40 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 45-41 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		

Table 45-41 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 45-42 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 45-43 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 45-44 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 45-45 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 45-46 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 45-46 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 45-47 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 45-48 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 45-49 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 45-50 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 45-51 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 45-51 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 45-52 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 45-53 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 45-54 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 45-55 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 45-56 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 45-56 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 45-57 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 45-58 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 45-59 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 45-60 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 45-61 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		

Table 45-61 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 45-62 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 45-63 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 45-64 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 45-65 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-66 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		

Table 45-66 PowerSupplyDcFailure (continued)

Alarm	Attributes	Applicable major release
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-67 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-68 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-69 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 45-70 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-71 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-72 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 45-73 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 45-74 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 45-75 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 45-76 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 45-77 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		

Table 45-77 RedundantMepMissing (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 45-78 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 45-79 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 45-80 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 6.4.4 • 6.4.5
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 45-81 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 45-82 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		

Table 45-82 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 45-83 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 45-84 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 45-85 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 45-86 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 45-87 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 45-87 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 45-88 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 45-89 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 45-90 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 45-91 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 45-92 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		

Table 45-92 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 45-93 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 45-94 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 45-95 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 45-96 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 45-97 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 45-98 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 45-99 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 45-100 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 45-101 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 45-102 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.4.3 • 6.4.4 • 6.4.5
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

46 OS6450

46.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 46-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 46-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 46-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 46-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 46-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 46-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 46-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 46-7 BITS2NotQualified

Alarm	Attributes	Applicable major release
Name: BITS2NotQualified (1941) Type: communicationsAlarm Package: sonet.BITS2NotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS2 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Input Administrative State' NOT EQUAL 'Down'))		

Table 46-7 BITS2NotQualified (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Input Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS2 is qualified		

Table 46-8 BITS2ReferenceLossOfSignal

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceLossOfSignal (9002) Type: communicationsAlarm Package: sonet.BITS2ReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceLossOfSignal	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS2 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS2 is properly configured.		

Table 46-9 BITS2ReferenceOutOfFrequency

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfFrequency (9003) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfFrequency	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS2 is correct.		

Table 46-10 BITS2ReferenceOutOfPollInRange

Alarm	Attributes	Applicable major release
Name: BITS2ReferenceOutOfPollInRange (9004) Type: communicationsAlarm Package: sonet.BITS2ReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITS2ReferenceOutOfPollInRange	Release: • 6.6.5 • 6.7.1

Table 46-10 BITS2ReferenceOutOfPollInRange (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the BITS2 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS2 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 46-11 BITSNotQualified

Alarm	Attributes	Applicable major release
Name: BITSNotQualified (547) Type: communicationsAlarm Package: sonet.BITSNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS/BITS1 timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Output Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Output Administrative State' EQUAL 'Down'))		
Remedial action: Make sure that BITS/BITS1 is qualified		

Table 46-12 BITSReferenceLossOfSignal (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceLossOfSignal (1950) Type: communicationsAlarm Package: sonet.BITSReferenceLossOfSignal Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceLossOfSignal	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS/BITS1 reference on an NE is not qualified due to Loss of Signal.		
Raising condition: (('Not Qualified Due To'anyBit'LOS'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'LOS')))		
Remedial action: Make sure that peer connected to BITS/BITS1 is properly configured.		

Table 46-13 BITSReferenceOutOfFrequency (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfFrequency (1951) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfFrequency Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfFrequency	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified due to Out of frequency.		
Raising condition: (('Not Qualified Due To'anyBit'OOF'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOF')))		
Remedial action: Make sure that frequency configured for BITS/BITS1 is correct.		

Table 46-14 BITSReferenceOutOfPollInRange (sonet)

Alarm	Attributes	Applicable major release
Name: BITSReferenceOutOfPollInRange (1952) Type: communicationsAlarm Package: sonet.BITSReferenceOutOfPollInRange Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BITSReferenceOutOfPollInRange	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the BITS/BITS1 Reference on an NE is not qualified state due to Out of poll in range.		
Raising condition: (('Not Qualified Due To'anyBit'OOPIR'))		
Clearing condition: NOT ((('Not Qualified Due To'anyBit'OOPIR')))		
Remedial action: Check the BITS/BITS1 is configured correctly. Check the SONET port is configured correctly and that the physical layer cabling is operating correctly. Contact your Nokia support representative if necessary		

Table 46-15 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		

Table 46-15 BootableConfigBackupFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 46-16 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 46-17 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		

Table 46-17 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 46-18 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 46-19 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 46-20 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 46-21 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 46-22 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		

Table 46-22 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 46-23 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 46-24 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 46-25 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 46-26 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 46-27 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1

Table 46-27 EquipmentDegraded (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 46-28 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 46-29 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 46-30 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 46-31 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 46-32 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		

Table 46-32 EthernetPortConfiguredLoopback (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 46-33 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 46-34 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 46-35 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 46-36 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 46-37 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1

Table 46-37 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 46-38 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 46-39 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		

Table 46-39 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 46-40 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 46-41 ExternalTimingReferenceNotQualified

Alarm	Attributes	Applicable major release
Name: ExternalTimingReferenceNotQualified (548) Type: communicationsAlarm Package: sonet.ExternalTimingReferenceNotQualified Raised on class: sonet.SiteSync	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: timingReferenceNotQualified	Release: • 6.6.5 • 6.7.1
Description: The alarm is raised when the External timing reference on an NE is not in the Qualified state.		
Raising condition: (('Qualified For Use' EQUAL 'Not Qualified') AND ('Administrative State' NOT EQUAL 'Down'))		
Clearing condition: (('Qualified For Use' NOT EQUAL 'Not Qualified') OR ('Administrative State' EQUAL 'Down'))		
Remedial action: Informational		

Table 46-42 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 46-43 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 46-44 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		

Table 46-44 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 46-45 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 46-46 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 46-47 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 46-48 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 46-49 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		

Table 46-49 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 46-50 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 46-51 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 46-52 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 46-53 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 46-54 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		

Table 46-54 LinkDown (equipment) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 46-55 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 46-56 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 46-57 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 46-58 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 46-59 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		

Table 46-59 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 46-60 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 46-61 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 46-62 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 46-63 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 46-64 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 46-65 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 46-66 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		

Table 46-66 NodeSuspended (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 46-67 NTPOperDown

Alarm	Attributes	Applicable major release
Name: NTPOperDown (4879) Type: communicationsAlarm Package: ntp.NTPOperDown Raised on class: ntp.NTP	Severity: info Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NTPOperDown	Release: • 6.6.5 • 6.7.1
Description: The alarm is generated when the NTP Operational State is down for NTP.		
Raising condition: (('Operational State' EQUAL 'Down') AND ('NTP State' EQUAL 'Enabled'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('NTP State' EQUAL 'Disabled'))		
Remedial action: Please check if NTP is administratively enabled (Admin State in NTP General Tab). If admin state down, enable it to make NTP operationally up.		

Table 46-68 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 46-69 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 46-70 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 46-71 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when persistence is set to Off in the NE BOF.		

Table 46-71 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 46-72 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 46-73 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		

Table 46-73 PortEtherSymMonSDAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 46-74 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 46-75 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-76 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-77 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-78 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: Generated when one of the chassis's power source supplies fails.		

Table 46-78 PowerSupplyInputFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-79 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 46-80 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-81 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-82 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 46-83 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		

Table 46-83 PrimaryImageBootFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 46-84 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 46-85 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 46-86 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 46-87 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 46-88 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1

Table 46-88 RemoteMepCCMAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 46-89 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 46-90 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 46-91 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 46-92 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 46-93 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 46-94 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 46-95 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 46-95 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 46-96 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 46-97 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 46-98 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 46-99 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 46-100 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		

Table 46-100 TmnxEqPortEtherLoopDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 46-101 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 46-102 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 46-102 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 46-103 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 46-104 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 46-105 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 46-106 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		

Table 46-106 UpgradedBuildVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 46-107 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 46-108 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 46-109 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 46-110 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 46-111 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.6.3 • 6.6.4 • 6.6.5 • 6.7.1
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		

Table 46-111 WrongCpaaSoftwareVersion (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

47 OS6850/6850E

47.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 47-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 47-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 47-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 47-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 47-4 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 47-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 47-6 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 47-7 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 47-8 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-9 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 47-10 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 47-11 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 47-12 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 47-13 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 47-14 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 47-15 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-15 ContainingEquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 47-16 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 47-17 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		

Table 47-17 CorruptImageFile (continued)

Alarm	Attributes	Applicable major release
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 47-18 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 47-19 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 47-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 47-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 47-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-22 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 47-23 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 47-24 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 47-25 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 47-26 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 47-27 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 47-28 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 47-29 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 47-30 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 47-31 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 47-32 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 47-33 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 47-34 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 47-35 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 47-36 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 47-37 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-37 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 47-38 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 47-39 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		

Table 47-39 IfVlanSubTypeConflict (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 47-40 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 47-41 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 47-42 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 47-43 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 47-44 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 47-45 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 47-46 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 47-47 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 47-48 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 47-49 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 47-50 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 47-51 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 47-52 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 47-53 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 47-54 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-54 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 47-55 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 47-56 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 47-57 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 47-58 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 47-59 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 47-60 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 47-61 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 47-62 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 47-63 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-63 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 47-64 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 47-65 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		

Table 47-65 PartialVPRNEncryption (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 47-66 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 47-67 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 47-68 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 47-69 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 47-70 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 47-71 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-72 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-73 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-74 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-75 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 47-76 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-77 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-78 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 47-79 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 47-80 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 47-81 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 47-82 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 47-83 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 47-84 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 47-85 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 47-86 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an RIP interface is operationally down.		

Table 47-86 RipInterfaceDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 47-87 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 47-88 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 47-88 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 47-89 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 47-90 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 47-91 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 47-92 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 47-93 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-93 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 47-94 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 47-95 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		

Table 47-95 TemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 47-96 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 47-97 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 47-98 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 47-99 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 47-99 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 47-100 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 47-101 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 47-102 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 47-103 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 47-104 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 47-105 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 47-106 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 47-107 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 47-107 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 47-108 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 47-109 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		

Table 47-109 VirtualNeighborDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 47-110 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.4.2 • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

48 OS6855

48.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 48-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 48-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 48-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 48-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 48-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 48-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 48-6 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 48-7 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when Bare Metal server is reachability down.		

Table 48-7 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 48-8 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-9 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 48-10 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 48-11 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 48-12 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 48-13 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 48-14 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		

Table 48-14 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 48-15 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 48-16 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 48-17 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 48-18 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 48-19 EfmOamAlarm

Alarm	Attributes	Applicable major release
Name: EfmOamAlarm (4617) Type: equipmentAlarm Package: ethernetequipment.EfmOamAlarm Raised on class: ethernetequipment.Dot3Oam	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EFMOAMOperationalstate-OutofService	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 48-19 EfmOamAlarm (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when EFM Ignore status is Enabled and EFM Operation Status has a fault that is not propagated to the Physical Port Operational State.		
Raising condition: ((('Operational Status' EQUAL 'Link Fault') OR ('Operational Status' EQUAL 'Active Send Local')) AND ('Ignore EFM State' EQUAL 'true'))		
Clearing condition: ((('Operational Status' NOT EQUAL 'Link Fault') AND ('Operational Status' NOT EQUAL 'Active Send Local')) OR ('Ignore EFM State' EQUAL 'false'))		
Remedial action: Informational - The alarm indicates that EFM has detected an error condition but has not affected the operation state of the port.		

Table 48-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 48-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 48-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 48-23 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 48-24 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		

Table 48-24 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 48-25 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 48-26 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 48-27 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 48-28 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 48-29 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 48-29 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 48-30 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 48-31 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		

Table 48-31 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 48-32 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 48-33 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 48-34 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 48-35 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 48-36 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		

Table 48-36 FanTrayRemoved (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 48-37 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 48-38 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 48-39 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 48-40 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 48-41 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		

Table 48-41 IgmpSnoopingDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 48-42 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 48-43 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 48-44 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 48-45 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 48-46 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the Lag Port Add function Fails.		

Table 48-46 LagPortAddFailed (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 48-47 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 48-48 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 48-49 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 48-50 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 48-51 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		

Table 48-51 LpsViolation (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 48-52 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 48-53 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 48-54 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 48-55 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 48-56 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		

Table 48-56 NeighborDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 48-57 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw.NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 48-58 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		

Table 48-58 NewSsh2ServerKeyDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 48-59 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 48-60 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 48-61 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 48-62 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 48-63 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		

Table 48-63 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 48-64 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 48-65 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 48-66 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 48-67 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 48-68 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 48-68 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 48-69 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 48-70 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		

Table 48-70 PortEtherSymMonSFAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 48-71 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-72 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-73 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-74 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-75 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		

Table 48-75 PowerSupplyInputFeedDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 48-76 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-77 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-78 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 48-79 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 48-80 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		

Table 48-80 RadiusOperStatusDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 48-81 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 48-82 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 48-83 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 48-84 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 48-85 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		

Table 48-85 RipDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 48-86 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 48-87 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 48-88 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 48-89 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 48-90 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 48-91 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 48-92 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		

Table 48-92 StatsRetrieveFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 48-93 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 48-94 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 48-95 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 48-96 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 48-97 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		

Table 48-97 TmnxEqPortEtherLoopDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 48-98 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 48-99 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 48-99 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band')))) **Remedial action:** A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 48-100 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 48-101 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 48-102 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 48-103 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		

Table 48-103 UpgradedBuildVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 48-104 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 48-105 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 48-106 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 48-107 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 48-108 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 48-108 VirtualLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 48-109 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 48-110 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

49 OS6860/OS6860E

49.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 49-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.2.1
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 49-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 8.2.1
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 49-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 8.2.1
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 49-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.2.1
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 49-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 8.2.1
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		

Table 49-5 AreaTypeMismatch (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 49-6 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.2.1
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 49-7 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 8.2.1
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 49-8 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-9 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 49-10 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		

Table 49-10 BootableConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 49-11 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 8.2.1
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 49-12 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 8.2.1
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 49-13 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 8.2.1
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 49-14 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment. ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdminist-rativelyDown	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 49-15 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 49-16 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 49-17 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 8.2.1
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 49-18 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 8.2.1
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		

Table 49-18 downgradedCardAlarm (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 49-19 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 49-20 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 8.2.1
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 49-21 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 8.2.1

Table 49-21 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 49-22 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 8.2.1
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 49-23 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 49-24 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 8.2.1
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 49-25 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 8.2.1
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 49-26 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 8.2.1
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		

Table 49-26 EthernetPortDuplicateLane (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 49-27 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.2.1
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 49-28 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 8.2.1
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 49-29 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 8.2.1
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 49-30 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 8.2.1
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 49-31 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 8.2.1

Table 49-31 EthernetPortNoFrameLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 49-32 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 8.2.1
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 49-33 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 8.2.1
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 49-34 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 8.2.1
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 49-35 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 8.2.1
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 49-36 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.2.1
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 49-37 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 8.2.1
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 49-38 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 8.2.1
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 49-39 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 8.2.1
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 49-40 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 49-41 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 49-42 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 8.2.1
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 49-43 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 8.2.1
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 49-44 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 49-45 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 8.2.1
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		

Table 49-45 LabelProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 49-46 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 8.2.1
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 49-47 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 8.2.1
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 49-48 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 8.2.1
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 49-49 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 8.2.1
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 49-50 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 8.2.1
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 49-51 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 8.2.1
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 49-52 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 49-53 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 8.2.1
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 49-54 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.2.1
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 49-55 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 49-56 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 49-57 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 8.2.1
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 49-58 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 8.2.1
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 49-59 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 8.2.1
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 49-60 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 8.2.1
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 49-61 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 8.2.1
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 49-62 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 49-63 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 8.2.1
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 49-64 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.2.1
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		

Table 49-64 OverTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 49-65 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 8.2.1
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 49-66 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 8.2.1
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 49-67 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 8.2.1
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 49-68 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 49-69 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		

Table 49-69 PollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 49-70 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 8.2.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 49-71 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 8.2.1
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 49-72 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 8.2.1
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-73 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 8.2.1
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-74 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 8.2.1
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-75 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 8.2.1
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-76 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 8.2.1
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 49-77 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 8.2.1
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-78 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 8.2.1
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-79 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 8.2.1
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 49-80 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 8.2.1
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 49-81 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 8.2.1
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 49-82 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 8.2.1
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 49-83 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 8.2.1
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		

Table 49-83 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 49-84 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 8.2.1
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 49-85 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 8.2.1
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 49-86 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 49-87 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 8.2.1
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 49-88 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 8.2.1
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 49-89 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 49-90 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 8.2.1
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 49-91 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 8.2.1
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		

Table 49-91 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 49-92 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 8.2.1
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 49-93 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 8.2.1
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 49-94 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 8.2.1
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 49-95 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 8.2.1
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 49-96 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 49-97 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.2.1
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 49-98 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 8.2.1
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 49-99 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 8.2.1
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		

Table 49-99 TemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 49-100 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 8.2.1
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 49-101 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 8.2.1
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 49-102 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 8.2.1
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 49-103 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 8.2.1
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		

Table 49-103 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 49-104 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 8.2.1
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 49-105 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 8.2.1
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 49-106 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 8.2.1
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 49-107 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 8.2.1
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 49-108 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 8.2.1
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 49-109 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 8.2.1
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 49-110 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 8.2.1
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 49-111 virtualChassisGroupStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisGroupStatusChange (9022) Type: equipmentAlarm Package: aosredundancy. virtualChassisGroupStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Group Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Group Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis Group consistency is Ok		

Table 49-112 virtualChassisHelloIntervalStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisHelloIntervalStatusChange (9023) Type: equipmentAlarm Package: aosredundancy. virtualChassisHelloIntervalStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Hello Interval Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Hello Interval Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Hello Interval consistency is Ok		

Table 49-113 virtualChassisIdStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisIdStatusChange (9024) Type: equipmentAlarm Package: aosredundancy. virtualChassisIdStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Id Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Id Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis ID consistency is OK		

Table 49-114 virtualChassisIpcVlanStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisIpcVlanStatusChange (9025) Type: equipmentAlarm Package: aosredundancy. virtualChassisIpcVlanStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('IPC Vlan Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('IPC Vlan Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC IpcVlan consistency is Ok		

Table 49-115 virtualChassisLicenseStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisLicenseStatusChange (9026) Type: equipmentAlarm Package: aosredundancy. virtualChassisLicenseStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('License Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('License Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC installed Licenceses consistency is Ok		

Table 49-116 virtualChassisRoleChange

Alarm	Attributes	Applicable major release
Name: virtualChassisRoleChange (9027) Type: equipmentAlarm Package: aosredundancy.virtualChassisRoleChange Raised on class: aosredundancy.AOSChassisState	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisRoleChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassisRole is changed from Master to Slave or Slave to Master.		
Raising condition: ('Role' EQUAL 'Master')		
Clearing condition: ('Role' EQUAL 'Slave')		
Remedial action: This Alarm can be cleared when the VC role Changes		

Table 49-117 virtualChassisTypeStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisTypeStatusChange (9028) Type: equipmentAlarm Package: aosredundancy. virtualChassisTypeStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 8.2.1
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Type Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Type Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis Type consistency is Ok		

Table 49-118 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 8.2.1
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 49-119 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 8.2.1
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 49-120 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 8.2.1
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		

Table 49-120 WrongCpaaSoftwareVersion (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

50 OS6900

50.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 50-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 50-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 50-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 50-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		

Table 50-4 AGWDiameterPeerDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 50-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 50-6 AtcaFanFailure

Alarm	Attributes	Applicable major release
Name: AtcaFanFailure (1124) Type: equipmentAlarm Package: equipment.AtcaFanFailure Raised on class: equipment.Fan	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('operationalState' EQUAL 'Disabled') OR ('operationalState' EQUAL 'Down'))		
Clearing condition: (('operationalState' EQUAL 'Enabled') OR ('operationalState' EQUAL 'Up'))		
Remedial action: This alarm is raised if the fan speed falls below 500 rpm. If the alarm persists, replace the appropriate (upper or lower) fan tray.		

Table 50-7 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 50-8 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 50-9 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-10 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 50-11 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 50-12 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 50-13 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 50-14 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 50-15 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-15 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 50-16 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 50-17 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 50-18 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation. AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 50-19 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 50-20 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 50-21 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 50-22 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-22 EquipmentDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 50-23 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 50-24 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 50-25 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 50-26 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 50-27 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 50-28 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 50-29 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 50-30 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 50-31 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 50-32 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 50-33 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 50-34 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 50-35 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 50-36 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 50-37 FrameSizeProblem (svt)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: svt.FrameSizeProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('Operational State' EQUAL 'MTU Mismatch') OR ('Operational State' EQUAL 'Tunnel MTU Too Small') OR ('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))		

Table 50-37 FrameSizeProblem (svt) (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' NOT EQUAL 'MTU Mismatch') AND ('Operational State' NOT EQUAL 'Tunnel MTU Too Small') AND NOT ((('State Cause'anyBit'Tunnel MTU Too Small') OR ('State Cause'anyBit'Service MTU Mismatch'))))		
Remedial action: The MTU value must be changed such that is is less than or equal to the supported MTU size value.		

Table 50-38 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 50-39 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 50-40 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 50-41 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 50-42 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-42 IgmpSnoopingDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 50-43 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 50-44 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		

Table 50-44 InterfaceDown (netw) (continued)

Alarm	Attributes	Applicable major release
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 50-45 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 50-46 LabelProblem

Alarm	Attributes	Applicable major release
Name: LabelProblem (98) Type: CircuitAlarm Package: svt.LabelProblem Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: labelProblem	Release: • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an ingress or an egress label is missing.		
Raising condition: (('Operational State' EQUAL 'No Egress Label') OR ('Operational State' EQUAL 'No Ingress Label') OR ('Operational State' EQUAL 'No Labels') OR ('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))		
Clearing condition: (('Operational State' NOT EQUAL 'No Egress Label') AND ('Operational State' NOT EQUAL 'No Ingress Label') AND ('Operational State' NOT EQUAL 'No Labels') AND NOT ((('State Cause'anyBit'No Egress VC Label') OR ('State Cause'anyBit'No Ingress VC Label') OR ('State Cause'anyBit'Label Manager Has Ran Out Of Labels'))))		
Remedial action: An ingress or egress label is missing for the SDP binding.		

Table 50-47 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 50-48 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 50-49 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 50-50 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 50-51 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 50-52 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 50-53 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 50-54 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 50-55 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		

Table 50-55 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 50-56 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 50-57 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 50-58 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 50-59 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 50-60 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 50-61 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 50-62 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 50-63 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 50-64 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 50-65 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 50-66 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 50-67 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 50-68 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 50-69 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 50-70 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 50-71 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 50-72 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment.PortEtherSymMonSFAlarm Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 50-73 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-74 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-75 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-76 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-77 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 50-78 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-79 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-80 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 50-81 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 50-82 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 50-83 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 50-84 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 50-85 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 50-86 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 50-87 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 50-88 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavailable	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 50-89 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 50-90 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 50-91 SdpBindingDown

Alarm	Attributes	Applicable major release
Name: SdpBindingDown (221) Type: SdpBindingAlarm Package: svt.SdpBindingDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpBindingNotReady	Release: • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an SDP binding has an Operational State other than Up.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-Homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For BGP Multi-Homing'))		
Remedial action: To resolve this alarm check the SDP binding to determine if a configuration mismatch exists. If configuration is determined to be correct then the associated network interface may be down. Further investigation is required to determine why the underlying network interface is down.		

Table 50-92 SdpBindingTunnelDown

Alarm	Attributes	Applicable major release
Name: SdpBindingTunnelDown (222) Type: CircuitAlarm Package: svt.SdpBindingTunnelDown Raised on class: svt.SdpBinding	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SdpTunnelNotReady	Release: • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an SDP binding tunnel has an Operational State other than Up.		

Table 50-92 SdpBindingTunnelDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Operational State' EQUAL 'Tunnel Not Ready') OR ('Operational State' EQUAL 'Tunnel Down') OR ('State Cause'anyBit'Tunnel Oper Down'))		
Clearing condition: (('Operational State' NOT EQUAL 'Tunnel Not Ready') AND ('Operational State' NOT EQUAL 'Tunnel Down') AND NOT (('State Cause'anyBit'Tunnel Oper Down')))		
Remedial action: To resolve this alarm check the endpoints of the SDP binding to determine if a configuration mismatch exists. If configuration matches then the underlying network resource between the endpoints of the SDP may be down. Further investigation is required to determine why the underlying transport network is down.		

Table 50-93 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 50-94 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		

Table 50-94 SiteManagementVlanConflict (continued)

Alarm	Attributes	Applicable major release
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 50-95 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 50-96 SpbSiteDown

Alarm	Attributes	Applicable major release
Name: SpbSiteDown (4396) Type: ProtocolAlarm Package: spb.SpbSiteDown Raised on class: spb.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an SPB site has an Operational State other than Up.		
Raising condition: ('Operational State' NOT EQUAL 'Up')		
Clearing condition: ('Operational State' EQUAL 'Up')		
Remedial action: Check if the administrative state is down. If the administrative state is up, then check the ISIS instance associated with the SPB and make sure it is up.		

Table 50-97 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 50-98 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 50-99 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 50-100 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 50-101 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 50-102 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 50-103 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-103 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 50-104 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		

Table 50-104 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 50-105 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 50-106 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 50-107 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 50-108 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 50-109 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 50-110 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 50-111 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4

Table 50-111 VersionConfigRestoreFailed (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 50-112 virtualChassisGroupStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisGroupStatusChange (9022) Type: equipmentAlarm Package: aosredundancy. virtualChassisGroupStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Group Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Group Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis Group consistency is Ok		

Table 50-113 virtualChassisHelloIntervalStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisHelloIntervalStatusChange (9023) Type: equipmentAlarm Package: aosredundancy. virtualChassisHelloIntervalStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Hello Interval Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Hello Interval Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Hello Interval consistency is Ok		

Table 50-114 virtualChassisIdStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisIdStatusChange (9024) Type: equipmentAlarm Package: aosredundancy. virtualChassisIdStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Id Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Id Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis ID consistency is OK		

Table 50-115 virtualChassisIpcVlanStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisIpcVlanStatusChange (9025) Type: equipmentAlarm Package: aosredundancy. virtualChassisIpcVlanStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('IPC Vlan Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('IPC Vlan Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC IpcVlan consistency is Ok		

Table 50-116 virtualChassisLicenseStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisLicenseStatusChange (9026) Type: equipmentAlarm Package: aosredundancy. virtualChassisLicenseStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('License Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('License Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC installed Licenceses consistency is Ok		

Table 50-117 virtualChassisRoleChange

Alarm	Attributes	Applicable major release
Name: virtualChassisRoleChange (9027) Type: equipmentAlarm Package: aosredundancy.virtualChassisRoleChange Raised on class: aosredundancy.AOSChassisState	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisRoleChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassisRole is changed from Master to Slave or Slave to Master.		
Raising condition: ('Role' EQUAL 'Master')		
Clearing condition: ('Role' EQUAL 'Slave')		
Remedial action: This Alarm can be cleared when the VC role Changes		

Table 50-118 virtualChassisTypeStatusChange

Alarm	Attributes	Applicable major release
Name: virtualChassisTypeStatusChange (9028) Type: equipmentAlarm Package: aosredundancy. virtualChassisTypeStatusChange Raised on class: aosredundancy.AOSChassisState	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: virtualChassisStatusChange	Release: • 7.3.3 • 7.3.4
Description: The alarm is raised when VirtualChassis status is changed from UP to Down.		
Raising condition: ('Chassis Type Consistency' EQUAL 'Inconsistent')		
Clearing condition: ('Chassis Type Consistency' EQUAL 'Consistent')		
Remedial action: This Alarm can be cleared when the VC Chassis Type consistency is Ok		

Table 50-119 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		

Table 50-119 VirtualLinkDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 50-120 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 50-121 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 7.2.1 • 7.3.1 • 7.3.2 • 7.3.3 • 7.3.4
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

51 OS9600

51.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 51-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 51-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 51-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 51-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 51-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		

Table 51-5 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 51-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 51-7 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-8 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 51-9 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 51-10 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3

Table 51-10 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 51-11 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 51-12 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 51-13 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministratively Down	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 51-14 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 51-15 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 51-15 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 51-16 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 51-17 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 51-18 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 51-19 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 51-20 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 51-21 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-22 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 51-23 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		

Table 51-23 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 51-24 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 51-25 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 51-26 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 51-27 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 51-28 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		

Table 51-28 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 51-29 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 51-30 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 51-31 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 51-32 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 51-33 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		

Table 51-33 EthernetPortSignalFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 51-34 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 51-35 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 51-36 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 51-37 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 51-38 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		

Table 51-38 IfVlanSubTypeConflict (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 51-39 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 51-40 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 51-41 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 51-42 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 51-43 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 51-43 IsisDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 51-44 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 51-45 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 51-46 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 51-47 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 51-48 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 51-48 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 51-49 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 51-50 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 51-51 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 51-52 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 51-53 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 51-53 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 51-54 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 51-55 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 51-56 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 51-57 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 51-58 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 51-58 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 51-59 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 51-60 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 51-61 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 51-62 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 51-63 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		

Table 51-63 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 51-64 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 51-65 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 51-66 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 51-67 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 51-68 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		

Table 51-68 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-69 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-70 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-71 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-72 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 51-73 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-74 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-75 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 51-76 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 51-77 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 51-78 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 51-79 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		

Table 51-79 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 51-80 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 51-81 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 51-82 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 51-83 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 51-84 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 51-84 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 51-85 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 51-86 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 51-87 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 51-88 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 51-89 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 51-89 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 51-90 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 51-91 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 51-92 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 51-93 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 51-94 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		

Table 51-94 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 51-95 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 51-96 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 51-97 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 51-98 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 51-99 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 51-100 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 51-101 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 51-102 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 51-103 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 51-104 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

52 OS9700

52.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 52-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 52-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 52-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 52-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 52-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		

Table 52-5 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 52-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 52-7 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-8 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 52-9 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 52-10 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3

Table 52-10 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 52-11 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 52-12 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 52-13 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 52-14 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 52-15 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 52-15 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 52-16 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 52-17 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 52-18 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 52-19 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 52-20 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 52-21 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-22 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 52-23 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		

Table 52-23 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 52-24 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 52-25 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 52-26 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 52-27 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 52-28 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		

Table 52-28 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 52-29 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 52-30 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 52-31 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoFrameLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 52-32 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment. EthernetPortRemoteFault Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 52-33 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		

Table 52-33 EthernetPortSignalFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 52-34 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 52-35 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 52-36 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 52-37 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 52-38 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		

Table 52-38 IfVlanSubTypeConflict (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 52-39 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 52-40 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 52-41 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 52-42 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 52-43 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 52-43 IsisDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 52-44 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 52-45 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 52-46 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 52-47 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 52-48 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 52-48 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 52-49 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 52-50 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 52-51 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 52-52 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 52-53 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 52-53 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 52-54 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 52-55 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 52-56 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 52-57 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 52-58 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 52-58 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 52-59 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 52-60 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 52-61 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 52-62 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 52-63 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		

Table 52-63 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 52-64 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 52-65 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 52-66 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 52-67 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 52-68 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		

Table 52-68 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-69 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-70 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-71 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-72 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 52-73 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-74 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-75 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 52-76 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 52-77 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 52-78 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 52-79 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		

Table 52-79 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 52-80 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 52-81 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 52-82 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 52-83 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 52-84 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 52-84 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 52-85 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 52-86 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 52-87 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 52-88 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 52-89 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 52-89 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 52-90 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 52-91 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 52-92 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 52-93 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 52-94 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		

Table 52-94 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 52-95 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 52-96 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 52-97 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 52-98 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 52-99 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 52-100 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 52-101 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 52-102 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 52-103 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 52-104 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

53 OS9700E/9800E

53.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 53-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 53-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		

Table 53-2 ActiveAbnormalCondition (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 53-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 53-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 53-5 AreaTypeMismatch

Alarm	Attributes	Applicable major release
Name: AreaTypeMismatch (38) Type: configurationAlarm Package: ospf.AreaTypeMismatch Raised on class: ospf.Area	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: areaTypeMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF area on one NE is configured as an NSSA and the same OSPF area on another NE is configured as a stub area.		
Raising condition: ('Type Mismatch' EQUAL 'true')		
Clearing condition: ('Type Mismatch' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The OSPF area type configured for the NE does not match with the same OSPF area configured on another NE. Compare the configuration on the endpoint and correct the mismatch.		

Table 53-6 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 53-7 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when Bare Metal server is reachability down.		

Table 53-7 BareMetalReachabilityDown (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 53-8 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-9 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 53-10 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 53-11 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 53-12 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 53-13 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 53-14 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministrativelyDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		

Table 53-14 ContainingEquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 53-15 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 53-16 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment. ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 53-17 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 53-18 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 53-19 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-19 EquipmentAdministrativelyDown (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 53-20 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 53-21 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 53-22 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-23 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 53-24 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 53-25 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 53-26 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		

Table 53-26 EthernetPortConfiguredLoopback (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 53-27 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment. EthernetPortDuplicateLane Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 53-28 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 53-29 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 53-30 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 53-31 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoBlockLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-31 EthernetPortNoBlockLock (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 53-32 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 53-33 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		

Table 53-33 EthernetPortRemoteFault (continued)

Alarm	Attributes	Applicable major release
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 53-34 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment. EthernetPortSignalFailure Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 53-35 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 53-36 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 53-37 ForwardingTableSizeLimitReached

Alarm	Attributes	Applicable major release
Name: ForwardingTableSizeLimitReached (164) Type: resourceAlarm Package: l2fwd.ForwardingTableSizeLimitReached Raised on class: l2fwd.SiteFib	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceLimitReached	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the number of MAC address entries in the FIB reaches or exceeds the VPLS site high watermark specified by l2fwd.SiteFib.highWatermark. The alarm clears when the number of MAC address entries in the FIB drops below the VPLS site low watermark specified by l2fwd.SiteFib.lowWatermark. The alarm can be raised against a VPLS site, L2 access interface, or spoke SDP binding.		
Raising condition: (('Entries' >=" 'Size') OR ('Entries' >= (('High Watermark' * 'Size') / 100.0)))"		
Clearing condition: (('Entries' < 'Size') AND (('High Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))) AND (('Low Watermark' EQUAL '0L') OR ('Entries' < (('Low Watermark' * 'Size') / 100.0))))		
Remedial action: Informational		

Table 53-38 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		

Table 53-38 FrameSizeProblem (netw) (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 53-39 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 53-40 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 53-41 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 53-42 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 53-43 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		

Table 53-43 IncompleteConfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 53-44 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 53-45 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 53-46 KeepAliveProblem

Alarm	Attributes	Applicable major release
Name: KeepAliveProblem (100) Type: oamAlarm Package: svt.KeepAliveProblem Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: keepAliveFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects a keep-alive protocol status of senderIdInvalid or responderIdError.		
Raising condition: (('Keep-Alive State' NOT EQUAL 'Disabled') AND ('Keep-Alive State' NOT EQUAL 'Alive') AND ('Keep-Alive State' NOT EQUAL 'Unknown'))		
Clearing condition: (('Keep-Alive State' EQUAL 'Disabled') OR ('Keep-Alive State' EQUAL 'Alive') OR ('Keep-Alive State' EQUAL 'Unknown'))		
Remedial action: Check the configuration of this tunnel and underlying physical transport.		

Table 53-47 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 53-48 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 53-49 LdpDown

Alarm	Attributes	Applicable major release
Name: LdpDown (22) Type: ProtocolAlarm Package: ldp.LdpDown Raised on class: ldp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an LDP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational state down reason and update accordingly.		

Table 53-50 LdpSessionNonexistent

Alarm	Attributes	Applicable major release
Name: LdpSessionNonexistent (2954) Type: LdpSessionAlarm Package: ldp.LdpSessionNonexistent Raised on class: ldp.Session	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LdpSessionDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an LDP session is non-existent.		
Raising condition: ('Session State' EQUAL 'Non-existent')		

Table 53-50 LdpSessionNonexistent (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Session State' EQUAL 'Operational')		
Remedial action: Please check the LDP session path to make sure all associated protocols/interfaces/connections are OK.		

Table 53-51 LdpTargetedPeerDown

Alarm	Attributes	Applicable major release
Name: LdpTargetedPeerDown (23) Type: ProtocolAlarm Package: ldp.LdpTargetedPeerDown Raised on class: ldp.TargetedPeer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an LDP targeted peer is operationally down.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: Please check the route to LDP targeted peer to make sure all associated protocols/interfaces/connections are OK.		

Table 53-52 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 53-53 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 53-54 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 53-55 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		

Table 53-55 LowTemperatureThresholdCrossed (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 53-56 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 53-57 LspDown

Alarm	Attributes	Applicable major release
Name: LspDown (25) Type: pathAlarm Package: mpls.LspDown Raised on class: mpls.Lsp	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lspDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the Operational State of an LSP is Down, but the Administrative State is Up.		
Raising condition: (('administrativeState' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('administrativeState' NOT EQUAL 'Up'))		
Remedial action: So many things can cause LSP down, check if source and destination interfaces are down, LSP path is down and the failure code, or MPLS path is down...		

Table 53-58 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 53-59 macMoveRateExceeded (svt)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: SpokeSdpBindingAlarm Package: svt.macMoveRateExceeded Raised on class: svt.SpokeSdpBinding	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SDP exceeds the Service Site's MAC Move Frequency.		
Raising condition: ('operationalFlags'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('operationalFlags'anyBit'Relearn Limit Exceeded'))		
Remedial action: Check Service Site MAC move frequency or underlying physical link to understand issue.		

Table 53-60 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		

Table 53-60 MepAISReceivedAlarm (continued)

Alarm	Attributes	Applicable major release
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 53-61 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 53-62 MplsDown

Alarm	Attributes	Applicable major release
Name: MplsDown (27) Type: ProtocolAlarm Package: mpls.MplsDown Raised on class: mpls.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an MPLS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: Check operational down reason and update accordingly.		

Table 53-63 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 53-64 NeighborDown

Alarm	Attributes	Applicable major release
Name: NeighborDown (121) Type: NeighborDown Package: ospf.NeighborDown Raised on class: ospf.AbstractNeighbor	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NeighborDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface neighbor is operationally Down.		
Raising condition: ('Operational State' NOT EQUAL 'full')		
Clearing condition: ('Operational State' EQUAL 'full')		
Remedial action: This alarm is raised when the OSPF interface neighbor is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 53-65 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-65 NeManagementAndTrapManagementMismatch (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 53-66 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 53-67 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-67 NodeDatabaseFallbackDetected (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 53-68 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 53-69 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 53-70 OspfInterfaceDown

Alarm	Attributes	Applicable major release
Name: OspfInterfaceDown (141) Type: OspfInterfaceDown Package: ospf.OspfInterfaceDown Raised on class: ospf.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: OspfInterfaceDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an OSPF interface is operationally down.		
Raising condition: ('operationalState' EQUAL 'Down')		
Clearing condition: ('operationalState' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 53-71 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 53-72 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-72 PartialResyncProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 53-73 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 53-74 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		

Table 53-74 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 53-75 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 53-76 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 53-77 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 53-78 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 53-79 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when an AC failure occurs on the power supply.		

Table 53-79 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-80 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-81 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-82 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-83 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 53-84 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		

Table 53-84 PowerSupplyOutputFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-85 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-86 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 53-87 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 53-88 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 53-89 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-89 ReachabilityProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 53-90 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam.RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 53-91 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		

Table 53-91 RedundantMepMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 53-92 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 53-93 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 53-94 RipInterfaceDown

Alarm	Attributes	Applicable major release
Name: RipInterfaceDown (11187) Type: InterfaceAlarm Package: rip.RipInterfaceDown Raised on class: rip.Interface	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: underlyingResourceUnavail-able	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an RIP interface is operationally down.		
Raising condition: ('Operational State' EQUAL 'Down')		
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the RIP interface is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 53-95 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 53-96 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-96 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 53-97 SdpEgressIfsNetDomainInConsistent

Alarm	Attributes	Applicable major release
Name: SdpEgressIfsNetDomainInConsistent (3616) Type: resourceAlarm Package: svt.SdpEgressIfsNetDomainInConsistent Raised on class: svt.Tunnel	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: sdpEgressIfsNetDomainIn-Consistent	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the SDP egress interface's consistency state changes to inconsistent.		
Raising condition: ('Egress Interfaces Consistency State' EQUAL '3')		
Clearing condition: ('Egress Interfaces Consistency State' EQUAL '2')		
Remedial action: To resolve this alarm check egress interfaces of the SDP configuration. If configuration is determined to be correct check underlying physical transport. Further investigation is required.		

Table 53-98 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		

Table 53-98 ServiceSiteDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 53-99 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 53-100 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 53-101 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 53-102 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 53-103 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-103 SubSysChassMemoryUsageHi (continued)

Alarm	Attributes	Applicable major release
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 53-104 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 53-105 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 53-106 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment.TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 53-107 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 53-108 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6

Table 53-108 TrapReceivingFailure (continued)

Alarm	Attributes	Applicable major release
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 53-109 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		

Table 53-109 TrapRoutePreferenceRedundancyMissing (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 53-110 TunnelAdministrativelyDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelAdministrativelyDown (523) Type: pathAlarm Package: svt.TunnelAdministrativelyDown Raised on class: svt.Tunnel	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelAdministrativelyDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is administratively down.		
Raising condition: ('administrativeState' NOT EQUAL 'Up')		
Clearing condition: ('administrativeState' EQUAL 'Up')		
Remedial action: Informational - an operator has manually turned down a service tunnel.		

Table 53-111 TunnelDown (svt)

Alarm	Attributes	Applicable major release
Name: TunnelDown (30) Type: pathAlarm Package: svt.TunnelDown Raised on class: svt.AbstractTunnel	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: tunnelDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 5620 SAM detects that a service tunnel is operationally down.		
Raising condition: (('Administrative' EQUAL 'Up') AND ('Operational' NOT EQUAL 'Up'))		
Clearing condition: (('Operational' EQUAL 'Up') OR ('Administrative' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that a problem has been made in the underlying transport network. If the alarm persists or re-occurs frequently then investigation of the underlying transport issues is warranted.		

Table 53-112 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 53-113 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 53-114 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		

Table 53-114 UpgradedBuildVersionMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 53-115 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 53-116 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 53-117 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 53-118 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 53-119 VirtualLinkDown

Alarm	Attributes	Applicable major release
Name: VirtualLinkDown (122) Type: VirtualLinkAlarm Package: ospf.VirtualLinkDown Raised on class: ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualLinkDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a virtual link is Down.		
Raising condition: ('Operational State' EQUAL 'Down')		

Table 53-119 VirtualLinkDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Operational State' NOT EQUAL 'Down')		
Remedial action: This alarm is raised when the OSPF virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 53-120 VirtualNeighborDown

Alarm	Attributes	Applicable major release
Name: VirtualNeighborDown (123) Type: VirtualNeighborDown Package: ospf.VirtualNeighborDown Raised on classes: • ospf.ShamLink • ospf.VirtualLink	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: VirtualNeighborDown	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when a neighbor virtual link is operationally down.		
Raising condition: ('neighborCount' EQUAL '0L')		
Clearing condition: ('neighborCount' NOT EQUAL '0L')		
Remedial action: This alarm is raised when the OSPF neighbor virtual link is operationally down. The situation may occur if the underlying physical interface is down either because of administrative disabling or a fault on the far end port or due to a cable connection or cable failure. This alarm will also be raised if the underlying transport network fails or is unreliable. Resolving the underlying instability in the transport network will correct this problem.		

Table 53-121 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.4.3 • 6.4.4 • 6.4.5 • 6.4.6
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		

54 OS9800

54.1 Alarms

Alarms

Note: Some alarms that the 5620 SAM can raise against this device may not be listed in this chapter. Associating alarms with specific NE types is an ongoing Alcatel-Lucent effort. If the 5620 SAM raises an alarm against this device type, and the alarm is not described in this chapter, see Chapter 39, “Unspecified NE”.

Table 54-1 AccessInterfaceDown

Alarm	Attributes	Applicable major release
Name: AccessInterfaceDown (249) Type: AccessInterfaceAlarm Package: service.AccessInterfaceDown Raised on class: service.AccessInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'Standby For MC-Ring') AND ('State Cause' NOT EQUAL 'Standby For MC Protocol') AND ('State Cause' NOT EQUAL 'Standby For BGP Multi-homing'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'Standby For MC-Ring') OR ('State Cause' EQUAL 'Standby For MC Protocol') OR ('State Cause' EQUAL 'Standby For BGP Multi-homing'))		
Remedial action: The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If neither appears to be the problem run diagnostics on the port to determine if it is faulty.		

Table 54-2 ActiveAbnormalCondition

Alarm	Attributes	Applicable major release
Name: ActiveAbnormalCondition (3938) Type: activeAbnormalConditionAlarm Package: netw.ActiveAbnormalCondition Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ActiveAbnormalConditionState	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is an indication for abnormal condition on NE.		
Raising condition: ('abnormalCondition' EQUAL 'true')		
Clearing condition: ('abnormalCondition' EQUAL 'false')		
Remedial action: This alarm is raised when there is a abnormal state indication on NE.		

Table 54-3 AggregatedVFLPortDown

Alarm	Attributes	Applicable major release
Name: AggregatedVFLPortDown (5436) Type: equipmentAlarm Package: equipment.AggregatedVFLPortDown Raised on class: equipment.Shelf	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: connectivityIssue	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is generated when the aggregated virtual fabric link on the virtual chassis slot is down.		
Raising condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' NOT EQUAL 'Up'))		
Clearing condition: (('Shelf Type' EQUAL '7850') AND ('Total Slots' EQUAL '4') AND ('Virtual Fabric Link State' EQUAL 'Up'))		
Remedial action: The alarm is raised when the aggregated virtual fabric link on the virtual chassis is down. Please check the virtual fabric links for the virtual chassis setup.		

Table 54-4 AGWDiameterPeerDown

Alarm	Attributes	Applicable major release
Name: AGWDiameterPeerDown (844) Type: EpcAlarm Package: lte.AGWDiameterPeerDown Raised on class: lte.AGWDiameterPeer	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Diameter peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 54-5 AuxiliaryServerStatus

Alarm	Attributes	Applicable major release
Name: AuxiliaryServerStatus (311) Type: communicationsAlarm Package: server.AuxiliaryServerStatus Raised on class: server.AuxiliaryServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server cannot communicate with an auxiliary server. The alarm clears when communication is restored.		
Raising condition: ('Server Status' EQUAL 'Down')		

Table 54-5 AuxiliaryServerStatus (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the AUX and SAM servers is unreliable.		

Table 54-6 BareMetalReachabilityDown

Alarm	Attributes	Applicable major release
Name: BareMetalReachabilityDown (10273) Type: virtualPortAlarm Package: dctr.BareMetalReachabilityDown Raised on class: dctr.BMDevice	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: BareMetalReachability-DownOrDeleted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when Bare Metal server is reachability down.		
Raising condition: (('bgpReachabilityState' NOT EQUAL '0'))		
Clearing condition: (('bgpReachabilityState' EQUAL '0'))		
Remedial action: This alarm can be cleared when bare metal device BGP prefix is up. Check for virtual switch controller down or virtual switch down or interface/port down in underlay network (hence the BGP prefix not advertised).		

Table 54-7 BgpDown

Alarm	Attributes	Applicable major release
Name: BgpDown (6) Type: ProtocolAlarm Package: bgp.BgpDown Raised on class: bgp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a BGP instance has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The BGP protocol entity is down - administratively disable BGP and re-enable. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-8 BootableConfigBackupFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigBackupFailed (103) Type: configurationAlarm Package: sw.BootableConfigBackupFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to back up a set of NE configuration files.		
Raising condition: ('Backup State' EQUAL 'Failure')		
Clearing condition: ('Backup State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: insufficient disk space is available to accommodate the NE configuration files (additional SAM platform alarms will accompany this alarm); the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 54-9 BootableConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: BootableConfigRestoreFailed (104) Type: configurationAlarm Package: sw.BootableConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM fails to restore a set of NE configuration files.		
Raising condition: ('Restore State' EQUAL 'Failure')		
Clearing condition: ('Restore State' EQUAL 'Success')		
Remedial action: Investigation is required to resolve the following possible scenarios: the NE is unreachable (including underlying transport network issue); loss of connectivity to the NE during transfer; the FTP daemon on the NE may have stopped; FTP security credential issues.		

Table 54-10 BootParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: BootParametersMisconfigured (35) Type: configurationAlarm Package: netw.BootParametersMisconfigured Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexFailure Applicable probable causes: • persistentIndexFailure • configFileBootFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3

Table 54-10 BootParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Description: The alarm is raised when the SNMP Index Boot Status on an NE is not set to Persistent.		
Raising condition: (('isGenericNode' EQUAL 'false') AND ('State' NOT EQUAL 'Pre-provisioned') AND ((('Config File Status' NOT EQUAL 'Executed Successfully') AND ('Config File Status' NOT EQUAL 'configFileStatus_unspecified')) OR (('Persistent Index Status' NOT EQUAL 'Rebuild Succeeded') AND ('Persistent Index Status' NOT EQUAL 'persistentIndexStatus_unspecified'))))		
Clearing condition: (('Config File Status' EQUAL 'Executed Successfully') AND ('Persistent Index Status' EQUAL 'Rebuild Succeeded'))		
Remedial action: Ensure that "SNMP Index Boot Status" is persistent (using cli command "show system information" on the NE). If not, unmanage the network element from SAM, ensure that "persist on" is set in the bof file, save the bof, save a config file, verify that an index file (.ndx) is saved as well, reboot the router, verify that SNMP Index Boot Status is persistent and finally remanage the router from SAM.		

Table 54-11 ClientDelegateServerStatus

Alarm	Attributes	Applicable major release
Name: ClientDelegateServerStatus (731) Type: communicationsAlarm Package: server.ClientDelegateServerStatus Raised on class: server.ClientDelegateServer	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: systemFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a client delegate server is unreachable.		
Raising condition: ('Server Status' EQUAL 'Down')		
Clearing condition: ('Server Status' EQUAL 'Up')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand why the connectivity between the client delegate platform and SAM servers is unreliable or the client delegate server itself is unreliable.		

Table 54-12 CmuManagementFailed

Alarm	Attributes	Applicable major release
Name: CmuManagementFailed (10040) Type: communicationsAlarm Package: lte.CmuManagementFailed Raised on class: lte.CompactMobilityUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ftpFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when SAM fails to manage a 9430 Compact Mobility Unit due to an FTP failure.		
Raising condition: ('Management State' EQUAL 'FTP Failed')		
Clearing condition: ('Management State' EQUAL 'Managed')		
Remedial action: Verify FTP connectivity between the 5620 SAM and the 9430 Compact Mobility Unit, then re-attempt to manage.		

Table 54-13 ContainingEquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentAdministrativelyDown (466) Type: equipmentAlarm Package: equipment.ContainingEquipmentAdministrativelyDown Raised on class: equipment.Port	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentAdministratively Down	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentAdministrativelyDown.		
Raising condition: (('Status' EQUAL 'Parent Admin Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Admin Down') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: Informational - no corrective action required.		

Table 54-14 ContainingEquipmentMismatch

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentMismatch (464) Type: equipmentAlarm Package: equipment.ContainingEquipmentMismatch Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentMismatch.		
Raising condition: (('Status' EQUAL 'Parent Type Mismatch') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Type Mismatch') OR ('isTerminatable' NOT EQUAL 'true'))		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 54-15 ContainingEquipmentOperationallyDown

Alarm	Attributes	Applicable major release
Name: ContainingEquipmentOperationallyDown (465) Type: equipmentAlarm Package: equipment.ContainingEquipmentOperationallyDown Raised on class: equipment.Port	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: containingEquipmentDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of containingEquipmentOperationllyDown.		
Raising condition: (('Status' EQUAL 'Parent Oper Down') AND ('isTerminatable' EQUAL 'true'))		
Clearing condition: (('Status' NOT EQUAL 'Parent Oper Down') OR ('isTerminatable' NOT EQUAL 'true'))		

Table 54-15 ContainingEquipmentOperationallyDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The operational state of the equipment element indicated in the alarm is down. This may be due to the element's administrative state or it may indicate that the element has failed.		

Table 54-16 CorruptImageFile

Alarm	Attributes	Applicable major release
Name: CorruptImageFile (171) Type: configurationAlarm Package: mediation.CorruptImageFile Raised on class: mediation.AbstractSoftwareFolderDescriptor	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: invalidOrCorruptImageFile	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more files in the 5620 SAM software image specified for a device software upgrade is invalid, corrupt or absent. The 5620 SAM validates a device software file set before it imports the file set and distributes it to an NE. Ensure that the file set downloads properly to the NE and is not tampered with before you re-attempt the upgrade. The alarm clears when a valid file set is on the NE and the 5620 SAM activates the software image in the file set.		
Raising condition: ('isImageValid' EQUAL 'false')		
Clearing condition: ('isImageValid' EQUAL 'true')		
Remedial action: The existing SW image in the SAM database should be replaced with an image that is known to be complete and valid.		

Table 54-17 downgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: downgradedCardAlarm (256) Type: softwareAlarm Package: equipment.downgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: downgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IOM is not upgraded or reset after a device software upgrade of both CPMs. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Downgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 54-18 EquipmentAdministrativelyDown

Alarm	Attributes	Applicable major release
Name: EquipmentAdministrativelyDown (455) Type: equipmentAlarm Package: equipment.EquipmentAdministrativelyDown Raised on class: equipment.Equipment	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentAdministratively-Down	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentAdministrativelyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Admin Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Admin Down')		
Remedial action: Informational - no corrective action required.		

Table 54-19 EquipmentDegraded

Alarm	Attributes	Applicable major release
Name: EquipmentDegraded (604) Type: equipmentAlarm Package: equipment.EquipmentDegraded Raised on class: equipment.FanTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: singleFanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a single fan fails. The chassis attempts to continue operating within the normal temperature range using only the remaining fans.		
Raising condition: ('Device State' EQUAL 'MinorFailure')		
Clearing condition: ('Device State' NOT EQUAL 'MinorFailure')		
Remedial action: The failed fan unit should be replaced.		

Table 54-20 EquipmentDown

Alarm	Attributes	Applicable major release
Name: EquipmentDown (10) Type: equipmentAlarm Package: equipment.EquipmentDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: inoperableEquipment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentOperationallyDown.		
Raising condition: ('compositeEquipmentState' EQUAL 'Oper Down')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Oper Down')		
Remedial action: This alarm indicates that a card in the NE has failed. The card must be replaced.		

Table 54-21 EquipmentFailure

Alarm	Attributes	Applicable major release
Name: EquipmentFailure (145) Type: equipmentAlarm Package: equipment.EquipmentFailure Raised on class: equipment.ReplaceableUnit	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: cardFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a I/O card or control processor or power-supply tray reports a failure. When the object type is ControlProcessor, a CPM may be unable to boot. When the object type is Power Supply Tray and the alarm is raised during device discovery, a power-supply tray may be out of service. When the object type is a Power Supply Tray and the device is in the managed state, a power-supply tray may be out of service or the AC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: ('operationalState' EQUAL 'Failed')		
Clearing condition: ('operationalState' NOT EQUAL 'Failed')		
Remedial action: If the alarm indicates that the CPM card or I/O card has a fault, remove the card and reset it. If this does not clear the alarm then please contact your Nokia support representative for assistance. If the alarm indicates that the Power Supply tray is out of service ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-22 EquipmentInTest

Alarm	Attributes	Applicable major release
Name: EquipmentInTest (11) Type: equipmentAlarm Package: equipment.EquipmentInTest Raised on class: equipment.Equipment	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentInTest	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when equipment enters a diagnostic state.		
Raising condition: ('compositeEquipmentState' EQUAL 'In Test')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'In Test')		
Remedial action: Informational - no corrective action required.		

Table 54-23 EquipmentMismatch

Alarm	Attributes	Applicable major release
Name: EquipmentMismatch (9) Type: equipmentAlarm Package: equipment.EquipmentMismatch Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentTypeMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMismatch.		

Table 54-23 EquipmentMismatch (continued)

Alarm	Attributes	Applicable major release
Raising condition: ('compositeEquipmentState' EQUAL 'Type Mismatch')		
Clearing condition: ('compositeEquipmentState' NOT EQUAL 'Type Mismatch')		
Remedial action: A configuration error has occurred which must be corrected. The card type configured for the slot identified in the alarm must match the installed card type.		

Table 54-24 EquipmentRemoved

Alarm	Attributes	Applicable major release
Name: EquipmentRemoved (8) Type: equipmentAlarm Package: equipment.EquipmentRemoved Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: replaceableEquipmentRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the compositeEquipmentState attribute has a value of equipmentMissing.		
Raising condition: ((('isEquipped' EQUAL 'false') OR ('compositeEquipmentState' EQUAL 'Removed')) AND ('isEquipmentInserted' EQUAL 'true'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Removed') AND ('isEquipped' EQUAL 'true'))		
Remedial action: Informational - this alarm is raised when a card is removed.		

Table 54-25 EthernetPortConfiguredLoopback

Alarm	Attributes	Applicable major release
Name: EthernetPortConfiguredLoopback (801) Type: configurationAlarm Package: ethernetequipment.EthernetPortConfiguredLoopback Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ethernetPortConfiguredLoopback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a timed loopback is in effect for an Ethernet port.		
Raising condition: (('Type' NOT EQUAL 'None'))		
Clearing condition: (('Type' EQUAL 'None'))		
Remedial action: This alarm has been raised bye the node because "Timed Loopback" option of the specific port's Ethernet property has been enabled. To resolve this problem from "Ethernet" tab of "Physical Port" properties form configure "Timed Loopback" Type property as "None".		

Table 54-26 EthernetPortDuplicateLane

Alarm	Attributes	Applicable major release
Name: EthernetPortDuplicateLane (3557) Type: communicationsAlarm Package: ethernetequipment.EthernetPortDuplicateLane Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: DuplicateLane	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a Duplicate Lane on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Duplicate Lane') AND ('Report Alarms'anyBit'Duplicate Lane')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 54-27 EthernetPortHighBer

Alarm	Attributes	Applicable major release
Name: EthernetPortHighBer (307) Type: communicationsAlarm Package: ethernetequipment.EthernetPortHighBer Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a high bit-error rate on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'High Bit Error Rate') AND ('Report Alarms'anyBit'High Bit Error Rate')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 54-28 EthernetPortLocalFault

Alarm	Attributes	Applicable major release
Name: EthernetPortLocalFault (305) Type: communicationsAlarm Package: ethernetequipment.EthernetPortLocalFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: LocalFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a local fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault'))		

Table 54-28 EthernetPortLocalFault (continued)

Alarm	Attributes	Applicable major release
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Local Fault') AND ('Report Alarms'anyBit'Local Fault')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 54-29 EthernetPortNoAmLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoAmLock (3558) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoAmLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoAmLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Am Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No AM Lock') AND ('Report Alarms'anyBit'No AM Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 54-30 EthernetPortNoBlockLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoBlockLock (3559) Type: communicationsAlarm Package: ethernetequipment. EthernetPortNoBlockLock Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoBlockLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a No Block Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Block Lock') AND ('Report Alarms'anyBit'No Block Lock')))		
Remedial action: One of the following conditions exists on the referenced physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault. If the problem cannot be resolved swap the card containing the port with a card which is known be functional.		

Table 54-31 EthernetPortNoFrameLock

Alarm	Attributes	Applicable major release
Name: EthernetPortNoFrameLock (306) Type: communicationsAlarm Package: ethernetequipment.EthernetPortNoFrameLock Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NoFrameLock	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports No Frame Lock on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'No Frame Lock') AND ('Report Alarms'anyBit'No Frame Lock')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 54-32 EthernetPortRemoteFault

Alarm	Attributes	Applicable major release
Name: EthernetPortRemoteFault (304) Type: communicationsAlarm Package: ethernetequipment.EthernetPortRemoteFault Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: RemoteFault	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a remote fault on an Ethernet port.		
Raising condition: (('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Remote Fault') AND ('Report Alarms'anyBit'Remote Fault')))		
Remedial action: One of the following conditions exists on the remote physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 54-33 EthernetPortSignalFailure

Alarm	Attributes	Applicable major release
Name: EthernetPortSignalFailure (303) Type: communicationsAlarm Package: ethernetequipment.EthernetPortSignalFailure Raised on class: ethernetequipment.EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: SignalFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device reports a signal failure on an Ethernet port.		

Table 54-33 EthernetPortSignalFailure (continued)

Alarm	Attributes	Applicable major release
Raising condition: (('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure'))		
Clearing condition: NOT ((('Outstanding Alarms'anyBit'Signal Failure') AND ('Report Alarms'anyBit'Signal Failure')))		
Remedial action: One of the following conditions exists on the physical interface which must be corrected. A cable/fiber fault exists which must be corrected - check to ensure that the cable is not faulty and is properly connected. The port is faulty - run diagnostics on the port to determine the nature of the fault.		

Table 54-34 FanFailure (equipment)

Alarm	Attributes	Applicable major release
Name: FanFailure (624) Type: equipmentAlarm Package: equipment.FanFailure Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fanFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the associated fan is not operationally Up.		
Raising condition: (('Device State' EQUAL 'Failed') OR ('Device State' EQUAL 'Unknown') OR ('Device State' EQUAL 'OutOfservice'))		
Clearing condition: ('Device State' EQUAL 'OK')		
Remedial action: Remove and reset the fan unit. If this does not resolve the problem replace the fan.		

Table 54-35 FanTrayRemoved

Alarm	Attributes	Applicable major release
Name: FanTrayRemoved (569) Type: equipmentAlarm Package: equipment.FanTrayRemoved Raised on class: equipment.FanTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: FanTrayRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the deviceState attribute has a value of deviceNotEquipped.		
Raising condition: ('Device State' EQUAL 'Not Equipped')		
Clearing condition: ('Device State' NOT EQUAL 'Not Equipped')		
Remedial action: Informational - a fan tray has been removed from the NE.		

Table 54-36 FrameSizeProblem (netw)

Alarm	Attributes	Applicable major release
Name: FrameSizeProblem (37) Type: configurationAlarm Package: netw.FrameSizeProblem Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: frameSizeProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a provisioned MTU size value is greater than the supported MTU size value.		
Raising condition: (('mtuMismatch' EQUAL 'true') AND ('portId' NOT EQUAL '0L'))		
Clearing condition: (('mtuMismatch' EQUAL 'false') OR ('portId' EQUAL '0L'))		
Remedial action: A configuration error has been made which must be corrected. The MTU value must be changed such that is less than or equal to the supported MTU size value.		

Table 54-37 GaPeerDown

Alarm	Attributes	Applicable major release
Name: GaPeerDown (3303) Type: EpcAlarm Package: lteggsn.GaPeerDown Raised on class: lteggsn.GaPeer	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EPSPeerDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the path management state of a Ga peer changes to a state other than Up.		
Raising condition: ('Path Management State' NOT EQUAL 'Active')		
Clearing condition: ('Path Management State' EQUAL 'Active')		
Remedial action: A Ga reference point (peer) is operationally down for one of the following reasons: the underlying IP or physical interface is down, the far end peer is down or the underlying transport between this NE and the peer NE is down. To resolve the issue ensure that the IP/physical interface is up, check that the far end peer is operational and check that the underlying transport network is up.		

Table 54-38 IfVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: IfVlanSubTypeConflict (213) Type: configurationAlarm Package: vlan.IfVlanSubTypeConflict Raised on class: vlan.L2AccessInterface	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service is configured with the same VLAN ID. The alarm is raised against an L2 access interface.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		

Table 54-38 IfVlanSubTypeConflict (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Interface.		

Table 54-39 IgmpDown

Alarm	Attributes	Applicable major release
Name: IgmpDown (158) Type: ProtocolAlarm Package: igmp.IgmpDown Raised on class: igmp.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IGMP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: While configured under VPRN, check if VPRN site is admin down, or if route distinguisher is not configured.		

Table 54-40 IgmpSnoopingDown

Alarm	Attributes	Applicable major release
Name: IgmpSnoopingDown (161) Type: ProtocolAlarm Package: layer2.IgmpSnoopingDown Raised on class: layer2.Bridge	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when IGMP snooping is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('IGMP Snooping' EQUAL 'Disabled')		
Clearing condition: ('IGMP Snooping' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable IGMP Snooping under the Bridge Instance.		

Table 54-41 IncompleteConfiguration

Alarm	Attributes	Applicable major release
Name: IncompleteConfiguration (1942) Type: operationalViolation Package: netw.IncompleteConfiguration Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: incompleteConfig	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a pre-provisioned NE has no objects configured beneath it.		
Raising condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' EQUAL '\"\"'))		
Clearing condition: (('State' EQUAL 'Pre-provisioned') AND ('eNodeB Equipment' NOT EQUAL '\"\"'))		
Remedial action: A configuration error has been made which must be corrected. The configuration of the pre-provisioned NE is incomplete. A work order was not associated with the pre-provisioned NE and as a consequence the attempt to auto-configure the NE failed.		

Table 54-42 InterfaceDown (netw)

Alarm	Attributes	Applicable major release
Name: InterfaceDown (36) Type: InterfaceAlarm Package: netw.InterfaceDown Raised on class: netw.StatefullConnectableInterface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: interfaceDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an interface or underlying resource fails, as indicated by an interface compositeState attribute value of failed or underlyingResourceFailed.		
Raising condition: (('compositeState' EQUAL 'Inoperable') OR ('compositeState' EQUAL 'Underlying Resource Inoperable'))		
Clearing condition: (('compositeState' NOT EQUAL 'Inoperable') AND ('compositeState' NOT EQUAL 'Underlying Resource Inoperable'))		
Remedial action: A physical port (physical interface, LAG, channel) associated with the network interface in not operational. Ensure that the interface is cabled and there are no configuration errors (i.e. MTU size set incorrectly etc) on the interface.		

Table 54-43 IsisDown

Alarm	Attributes	Applicable major release
Name: IsisDown (19) Type: ProtocolAlarm Package: isis.IsisDown Raised on class: isis.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an IS-IS site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		

Table 54-43 IsisDown (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The protocol is not working anymore, could be a problem with IP addresses, resources on the device, ...		

Table 54-44 LagDown

Alarm	Attributes	Applicable major release
Name: LagDown (20) Type: equipmentAlarm Package: lag.LagDown Raised on class: lag.Interface	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: lagDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all ports in a LAG are operationally down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('operationalState' NOT EQUAL 'Up'))		
Clearing condition: (('operationalState' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This alarm indicates that all physical Ethernet links associated with a LAG are operationally down. The reasons for the links to be down may vary from link to link. The following possible causes of this alarm should be investigated. The physical port (near end or far end may have failed - this can be remedied by replacing the interface card in question. The physical links may have been turned down administratively - re-enable the links. A cable failure or disconnect may have occurred - please ensure that the cables are properly connected to the physical port and and that the cable has not been damaged.		

Table 54-45 LagPortAddFailed

Alarm	Attributes	Applicable major release
Name: LagPortAddFailed (422) Type: equipmentAlarm Package: equipment.LagPortAddFailed Raised on class: equipment.PhysicalPort	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: linkDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the Lag Port Add function Fails.		
Raising condition: (('state' EQUAL 'Link Down') AND ('LAG ID' > '0'))		
Clearing condition: (('state' NOT EQUAL 'Link Down') OR ('LAG ID' EQUAL '0'))		
Remedial action: A configuration error has occurred which must be corrected. The link that was to be added to the LAG group may be of the wrong type (i.e. non ethernet) or the limit of the number of links supported in a LAG may have been reached.		

Table 54-46 LicensedLimitExceeded

Alarm	Attributes	Applicable major release
Name: LicensedLimitExceeded (127) Type: licensingAlarm Package: security.LicensedLimitExceeded Raised on class: security.SamLicensePoints	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: licensedLimitExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the license items in the network exceeds 100 percent of the license capacity.		
Raising condition: ('Exceeded' EQUAL 'true')		
Clearing condition: ('Exceeded' NOT EQUAL 'true')		
Remedial action: Informational - The number of SAM licenses purchased and available on the SAM server is insufficient as compared to the number of NEs/MDA/Cells under management in the network. Please contact your Nokia sales representative to purchase additional licenses.		

Table 54-47 LinkDown (equipment)

Alarm	Attributes	Applicable major release
Name: LinkDown (12) Type: communicationsAlarm Package: equipment.LinkDown Raised on class: equipment.Equipment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: portLinkProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a port has no associated physical link or remote end point is operationally down.		
Raising condition: (('compositeEquipmentState' EQUAL 'Link Down') OR ('compositeEquipmentState' EQUAL 'Oper Down'))		
Clearing condition: (('compositeEquipmentState' NOT EQUAL 'Link Down') AND ('compositeEquipmentState' NOT EQUAL 'Oper Down'))		
Remedial action: Please make sure that port has physical link and remote end point is operationally up.		

Table 54-48 LowTemperatureDetected

Alarm	Attributes	Applicable major release
Name: LowTemperatureDetected (1127) Type: environmentalAlarm Package: equipment.LowTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature falls below the minimum threshold.		
Raising condition: ('Low Temperature State' EQUAL 'Low')		
Clearing condition: ('Low Temperature State' NOT EQUAL 'Low')		

Table 54-48 LowTemperatureDetected (continued)

Alarm	Attributes	Applicable major release
Remedial action: The NE has detected internal temperatures which are abnormally low. This may happen when the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 54-49 LowTemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: LowTemperatureThresholdCrossed (1128) Type: environmentalAlarm Package: equipment. LowTemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOvercooled	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a low-temperature threshold is crossed.		
Raising condition: ('lowTemperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('lowTemperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 54-50 LpsViolation

Alarm	Attributes	Applicable major release
Name: LpsViolation (518) Type: learnedPortSecurityAlarm Package: lps.LpsViolation Raised on class: lps.LearnedPortSecurity	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: learnedPortSecurityViolation	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an LPS violation.		
Raising condition: ('Operational State' EQUAL 'Security Violated')		
Clearing condition: ('Operational State' EQUAL 'Down')		
Remedial action: Port reset is required to return the port to normal operation.		

Table 54-51 macMoveRateExceeded (service)

Alarm	Attributes	Applicable major release
Name: macMoveRateExceeded (3690) Type: accessInterfaceAlarm Package: service.macMoveRateExceeded Raised on class: service.AccessInterface	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: MacMoveRateExceeded	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the SAP exceeds the MAC Move Frequency of the service site.		
Raising condition: ('State Cause'anyBit'Relearn Limit Exceeded')		
Clearing condition: NOT (('State Cause'anyBit'Relearn Limit Exceeded'))		
Remedial action: Informational.		

Table 54-52 MepAISReceivedAlarm

Alarm	Attributes	Applicable major release
Name: MepAISReceivedAlarm (2945) Type: oamAlarm Package: ethernetoam.MepAISReceivedAlarm Raised on class: ethernetoam.Mep	Severity: indeterminate Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP receives AIS test frames from one or more of its sub-layer MEPs.		
Raising condition: (('AIS Received (AisRx)' EQUAL 'true') AND ('Facility VLAN ID' EQUAL '0'))		
Clearing condition: ('AIS Received (AisRx)' EQUAL 'false')		
Remedial action: This alarm indicates that it has received a MEP fault from a sub-layer MEP, user should investigate the fault cause on the sub-layer MEP and resolve this root cause issue.		

Table 54-53 MobileConnectorDown

Alarm	Attributes	Applicable major release
Name: MobileConnectorDown (1064) Type: EpcAlarm Package: lteservice.MobileConnectorDown Raised on class: lteservice.MobileServiceConnector	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: EpcDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM no longer manages the EPS path instance of this mobile service site. As a result, the service must be regenerated.		
Raising condition: ('EPS Path' EQUAL '\"\"')		
Clearing condition: ('EPS Path' NOT EQUAL '\"\"')		

Table 54-53 MobileConnectorDown (continued)

Alarm	Attributes	Applicable major release
Remedial action: The underlying transport network has gone down resulting in the deletion of a mobile service connector (EPS path). Correct the issue with the transport network and regenerate the mobile service connector by clicking on the re-calculate button on the mobile service properties form.		

Table 54-54 MvrSiteDown

Alarm	Attributes	Applicable major release
Name: MvrSiteDown (162) Type: ProtocolAlarm Package: layer2.MvrSiteDown Raised on class: layer2.MvrSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('MVR Admin Status' EQUAL 'Disabled')		
Clearing condition: ('MVR Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable MVR Admin Status under the Bridge Instance.		

Table 54-55 NeManagementAndTrapManagementMismatch

Alarm	Attributes	Applicable major release
Name: NeManagementAndTrapManagementMismatch (1079) Type: communicationsAlarm Package: netw. NeManagementAndTrapManagementMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: neManagementChange	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE configuration is one of the following: - The Active Management IP is set to Out Of Band, and the Primary Route Preference is set to In Band. - The Active Management IP is set to In Band, and the Primary Route Preference is set to Out of Band.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'Out Of Band')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND (('Management IP Selection' EQUAL 'In Band Preferred') OR ('Management IP Selection' EQUAL 'In Band Only')) AND ('Primary Route Preference' EQUAL 'In Band')) OR (('Active Management IP' EQUAL 'Out Of Band') AND (('Management IP Selection' EQUAL 'Out Of Band Preferred') OR ('Management IP Selection' EQUAL 'Out Of Band Only')) AND ('Primary Route Preference' EQUAL 'Out Of Band')))		
Remedial action: A configuration error has been made which must be corrected. The parameters described in the description for this alarm must match.		

Table 54-56 NewSsh2ServerKeyDetected

Alarm	Attributes	Applicable major release
Name: NewSsh2ServerKeyDetected (285) Type: communicationsAlarm Package: security.NewSsh2ServerKeyDetected Raised on class: security.KnownHostKey	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ssh2ServerKeyMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a 5620 SAM main server detects a new public SSH key.		
Raising condition: ('SSH2 Server Key Status' EQUAL 'Mismatch SSH2 Host Key')		
Clearing condition: ('SSH2 Server Key Status' EQUAL 'Active SSH2 Host Key')		
Remedial action: Informational - possible security breach. The SSH key of the router is different from the one known to the SAM server.		

Table 54-57 NodeDatabaseFallbackDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseFallbackDetected (2923) Type: communicationsAlarm Package: netw.NodeDatabaseFallbackDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseFallback	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration fallback is detected on the node and comes back up with a previous configuration. To correct this situation it might be necessary to reconfigure the node, or perform full resync its database with the 'fallback' configuration returned by the node.		
Raising condition: ('State' EQUAL 'Node Configuration Fallback')		
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE has come back to a previous configuration. Perform a manual Full Resync or a Reconfigure of the NE		

Table 54-58 NodeDatabaseMisalignmentDetected

Alarm	Attributes	Applicable major release
Name: NodeDatabaseMisalignmentDetected (2924) Type: communicationsAlarm Package: netw.NodeDatabaseMisalignmentDetected Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: nodeDatabaseMisalignment	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a configuration misalignment has been detected on the node and comes back up with an unexpected configuration (configuration change triggered by external tool) To correct this situation it might be necessary to reconfigure the node with the 5620 SAM's old configuration or accept the new configuration received from the node.		
Raising condition: ('State' EQUAL 'Node Configuration Misalignment')		

Table 54-58 NodeDatabaseMisalignmentDetected (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('State' EQUAL 'Managed')		
Remedial action: the NE configuration is misaligned. Perform a resync in order to update SAM configuration according to the NE.		

Table 54-59 NodeSuspended

Alarm	Attributes	Applicable major release
Name: NodeSuspended (5123) Type: communicationsAlarm Package: netw.NodeSuspended Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: NodeSuspend	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM detects an NE moved to suspend state as per user request.		
Raising condition: ('SNMP Reachability' EQUAL 'Suspended')		
Clearing condition: ('SNMP Reachability' NOT EQUAL 'Suspended')		
Remedial action: This alarm is raised when user suspends the network element.The alarm will be cleared when the network element is managed back.		

Table 54-60 OverTemperatureDetected

Alarm	Attributes	Applicable major release
Name: OverTemperatureDetected (388) Type: environmentalAlarm Package: equipment.OverTemperatureDetected Raised on class: equipment.Shelf	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the chassis temperature exceeds the maximum threshold value.		
Raising condition: ('Over Temperature State' EQUAL 'Over')		
Clearing condition: ('Over Temperature State' NOT EQUAL 'Over')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 54-61 PartialResyncProblem

Alarm	Attributes	Applicable major release
Name: PartialResyncProblem (4401) Type: communicationsAlarm Package: netw.PartialResyncProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: partialResyncProblem	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a partial resync on an NE fails. For example, when resyncing only some MIB entries as opposed to a full resync. The periodic reachability test (sysUpTime) is not considered a partial resync, neither is a full resync. However, a PartialResyncProblem alarm can only be reset by a FullResync.		
Raising condition: ('partialResyncStatus' EQUAL 'Partial Resync Failed')		
Clearing condition: ('partialResyncStatus' EQUAL 'Partial Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE.		

Table 54-62 PartialVPRNEncryption

Alarm	Attributes	Applicable major release
Name: PartialVPRNEncryption (8992) Type: configurationAlarm Package: nge.PartialVPRNEncryption Raised on class: nge.VprnEncryptService	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConfigMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when one or more sites are not encryption enabled in a VPRN service.		
Raising condition: (('VPRN Service Encryption Status' EQUAL 'Partial'))		
Clearing condition: (('VPRN Service Encryption Status' NOT EQUAL 'Partial'))		
Remedial action: This site is newly added to the VPRN service, Perform the encrypt operation on the KeyGroup to clear the alarm.		

Table 54-63 PersistentIndexParametersMisconfigured

Alarm	Attributes	Applicable major release
Name: PersistentIndexParametersMisconfigured (173) Type: configurationAlarm Package: netw. PersistentIndexParametersMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: persistentIndexConfiguration-Mismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when persistence is set to Off in the NE BOF.		
Raising condition: (('Persistent SNMP Indices' EQUAL 'False') OR (('hasRedundantProcessorCards' EQUAL 'true') AND ('Redundant Synchronization Mode' EQUAL 'None')))		

Table 54-63 PersistentIndexParametersMisconfigured (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('Persistent SNMP Indices' EQUAL 'True') AND (('hasRedundantProcessorCards' EQUAL 'false') OR ('Redundant Synchronization Mode' NOT EQUAL 'None')))		
Remedial action: A configuration error has occurred that must be corrected. Use the CLI on the NE to enable persistency in the BOF. The discovery process will complete on the next discovery scan. A re-scan can be triggered immediately for the NE from within the discovery manager		

Table 54-64 PimDown

Alarm	Attributes	Applicable major release
Name: PimDown (184) Type: ProtocolAlarm Package: pim.PimDown Raised on class: pim.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a PIM site is administratively Up but operationally Down. The alarm is cleared when the PIM site becomes operationally Up but administratively Down.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: This should never happen. Contact your Nokia support representative for assistance.		

Table 54-65 PollerProblem

Alarm	Attributes	Applicable major release
Name: PollerProblem (31) Type: communicationsAlarm Package: netw.PollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Resync Status' EQUAL 'Full Resync Failed')		
Clearing condition: ('Resync Status' EQUAL 'Full Resync Done')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 54-66 PortEtherSymMonSDAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSDAlarm (5662) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSDAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSDThrehol-dExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Degradation Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SD Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SD Threshold Exceeded')		
Remedial action: Symbol monitor signal degradation alarm could be cleared by changing/disabling the associated threshold/multiplier values or it is self clearing and will clear once the error rate drops below 1/10th of the configured rate.		

Table 54-67 PortEtherSymMonSFAlarm

Alarm	Attributes	Applicable major release
Name: PortEtherSymMonSFAlarm (5663) Type: communicationsAlarm Package: ethernetequipment. PortEtherSymMonSFAlarm Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: etherPortSymMonSFThrehold-ExceededAlarm	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Ethernet port Symbol Monitor Failure alarm condition is detected (Signal Failure Threshold exceeded).		
Raising condition: ('Symbol Alarm Reason' EQUAL 'SF Threshold Exceeded')		
Clearing condition: ('Symbol Alarm Reason' NOT EQUAL 'SF Threshold Exceeded')		
Remedial action: Symbol monitor signal failure alarm could be cleared by changing/disabling the associated threshold/multiplier values or by taking the port out of service (eg. shutdown, card/mda reset, physical link loss).		

Table 54-68 PowerSupplyAcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyAcFailure (9644) Type: equipmentAlarm Package: equipment.PowerSupplyAcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyAcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when an AC failure occurs on the power supply.		
Raising condition: ('AC Voltage Status' EQUAL 'Out of Range')		

Table 54-68 PowerSupplyAcFailure (continued)

Alarm	Attributes	Applicable major release
Clearing condition: (('AC Voltage Status' EQUAL 'Not Equipped') OR ('AC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-69 PowerSupplyDcFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyDcFailure (9645) Type: equipmentAlarm Package: equipment.PowerSupplyDcFailure Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyDcFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a DC failure occurs on the power supply.		
Raising condition: ('DC Voltage Status' EQUAL 'Out of Range')		
Clearing condition: (('DC Voltage Status' EQUAL 'Not Equipped') OR ('DC Voltage Status' EQUAL 'OK'))		
Remedial action: Insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-70 PowerSupplyFailure (equipment)

Alarm	Attributes	Applicable major release
Name: PowerSupplyFailure (633) Type: equipmentAlarm Package: equipment.PowerSupplyFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a power-supply tray reports a failure. When the alarm is raised during device discovery, a power-supply tray may be out of service. When the alarm is raised while the device is in the managed state, a power-supply tray may be out of service or the AC or DC power shelf has a fault condition. The alarm clears when the status changes to OK.		
Raising condition: (('Power Supply 1 Status' EQUAL 'Not Equipped') OR ('Power Supply 1 Status' EQUAL 'Failed'))		
Clearing condition: (('Power Supply 1 Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-71 PowerSupplyInputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFailure (9622) Type: equipmentAlarm Package: equipment.PowerSupplyInputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power source supplies fails.		
Raising condition: ('Power Supply Input Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Input Status' EQUAL 'Not Equipped') OR ('Power Supply Input Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-72 PowerSupplyInputFeedDown

Alarm	Attributes	Applicable major release
Name: PowerSupplyInputFeedDown (5422) Type: equipmentAlarm Package: equipment.PowerSupplyInputFeedDown Raised on class: equipment.PowerSupplyTray	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyInputFeedDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is generated if any one of the input feeds for a given power supply is not supplying power.		
Raising condition: (('inputFeedStatus' EQUAL 'Input A Down') OR ('inputFeedStatus' EQUAL 'Input B Down') OR (('inputFeedStatus'allBits'Input A Down') AND ('inputFeedStatus'allBits'Input B Down')))		
Clearing condition: ('inputFeedStatus' EQUAL 'None')		
Remedial action: Restore all of the input feeds that are not supplying power.		

Table 54-73 PowerSupplyOutputFailure

Alarm	Attributes	Applicable major release
Name: PowerSupplyOutputFailure (9623) Type: equipmentAlarm Package: equipment.PowerSupplyOutputFailure Raised on class: equipment.PowerSupplyTray	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOutputFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: Generated when one of the chassis's power output fails.		
Raising condition: ('Power Supply Output Status' EQUAL 'Failed')		
Clearing condition: (('Power Supply Output Status' EQUAL 'Not Equipped') OR ('Power Supply Output Status' EQUAL 'OK'))		
Remedial action: Ensure that the NE is properly connected to power. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-74 PowerSupplyOverTemperature

Alarm	Attributes	Applicable major release
Name: PowerSupplyOverTemperature (9646) Type: equipmentAlarm Package: equipment.PowerSupplyOverTemperature Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: powerSupplyOverTemperature	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This notification is generated when a power supply temperature surpasses the threshold of the particular physical chassis.		
Raising condition: ('Temperature Status' EQUAL 'Out of Range')		
Clearing condition: (('Temperature Status' EQUAL 'Not Equipped') OR ('Temperature Status' EQUAL 'OK'))		
Remedial action: Check input feed and/or insert a new power supply. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-75 PowerSupplyRemoved

Alarm	Attributes	Applicable major release
Name: PowerSupplyRemoved (542) Type: equipmentAlarm Package: equipment.PowerSupplyRemoved Raised on class: equipment.PowerSupplyTray	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: PowerSupplyRemoved	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a chassis power supply is removed.		
Raising condition: ('Power Supply 1 Status' EQUAL 'Not Equipped')		
Clearing condition: ('Power Supply 1 Status' NOT EQUAL 'Not Equipped')		
Remedial action: To recover from this event, the customer is requested to add a new power supply to the system, or change a faulty power supply with a working one.		

Table 54-76 PrimaryImageBootFailure

Alarm	Attributes	Applicable major release
Name: PrimaryImageBootFailure (191) Type: configurationAlarm Package: sw.PrimaryImageBootFailure Raised on class: sw.CardSoftware	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: bootOptionFileMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the primary software image specified in an NE BOF is unusable.		
Raising condition: (('imageSource' NOT EQUAL 'Primary') AND ('imageSource' NOT EQUAL 'Unknown'))		
Clearing condition: (('imageSource' EQUAL 'Primary') OR ('imageSource' EQUAL 'Unknown'))		
Remedial action: The SW image on the NE may have been inadvertently corrupted. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 54-77 RadiusOperStatusDown

Alarm	Attributes	Applicable major release
Name: RadiusOperStatusDown (3692) Type: radiusOperStatusDownAlarm Package: netw.RadiusOperStatusDown Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: radiusOperationStatusDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all RADIUS servers have gone down.		
Raising condition: ('Global RADIUS Operational State' EQUAL 'Down')		
Clearing condition: ('Global RADIUS Operational State' EQUAL 'Up')		
Remedial action: Verify the RADIUS server is properly configured and radius server state is up.Check the connectivity between SAM server and radius server configured on the Network element.		

Table 54-78 ReachabilityProblem

Alarm	Attributes	Applicable major release
Name: ReachabilityProblem (243) Type: communicationsAlarm Package: netw.ReachabilityProblem Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ReachabilityTestFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a mediation poll of the SysUpTimeAlarm object on an NE fails, for example, because of network congestion or because the NE is too busy to respond. The probable cause is an unreachable NE Mediation agent on the NE. The polling interval depends on the NE type and is configurable in nms-server.xml. By default, the 5620 SAM polls a managed NE every four minutes. If a poll fails, the alarm is raised. The alarm clears when the 5620 SAM receives a response from the NE, and the 5620 SAM GUI icon that represents the NE turns from red to green.		
Raising condition: ('SNMP Reachability' EQUAL 'Down')		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 54-79 RedundantMepMisconfiguration

Alarm	Attributes	Applicable major release
Name: RedundantMepMisconfiguration (3631) Type: oamAlarm Package: ethernetoam. RedundantMepMisconfiguration Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: misconfiguredRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an Active and Redundant MEP do not have the same ID, Operational MAC Address or Sub Group configured.		
Raising condition: ('validRedundantMepConfig' EQUAL 'false')		

Table 54-79 RedundantMepMisconfiguration (continued)

Alarm	Attributes	Applicable major release
Clearing condition: ('validRedundantMepConfig' EQUAL 'true')		
Remedial action: MC-LAG redundant MEP configuration (MEP ID or Mac Address) for Active & Standby Interfaces do not match, this could cause issues with CFM or CCM tests if Active interface changes. Delete and Re-create Standby MEP to match Active.		

Table 54-80 RedundantMepMissing

Alarm	Attributes	Applicable major release
Name: RedundantMepMissing (3632) Type: oamAlarm Package: ethernetoam.RedundantMepMissing Raised on class: ethernetoam.Mep	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRedundantMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP misses a redundant counterpart on LAG or SAP.		
Raising condition: (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' EQUAL '\"\"'))		
Clearing condition: (('MC-LAG Inactive' EQUAL 'Not Applicable') OR (('MC-LAG Inactive' NOT EQUAL 'Not Applicable') AND ('Redundant MEP' NOT EQUAL '\"\"')))		
Remedial action: MC-LAG redundant MEP is missing Active & Standby Interfaces, this will cause issues with CFM or CCM tests if Active interface changes. Create missing Active/Standby MEP to match existing.		

Table 54-81 RemoteMepCCMAlarm

Alarm	Attributes	Applicable major release
Name: RemoteMepCCMAlarm (502) Type: oamAlarm Package: ethernetoam.RemoteMepCCMAlarm Raised on class: ethernetoam.Mep	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: missingRemoteMep	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a MEP loses connectivity with one or more remote MEPs. The Remote MEP DB State tab on a MEP lists the missing remote MEPs.		
Raising condition: ('High-Priority Defect' NOT EQUAL '0')		
Clearing condition: ('High-Priority Defect' EQUAL '0')		
Remedial action: MEP has lost communication with Remote MEP defined in Maintenance Association (MEG) Remote MEP list, Either Remote MEP list is incorrect or diagnose connection fault and resolve.		

Table 54-82 RipDown

Alarm	Attributes	Applicable major release
Name: RipDown (72) Type: ProtocolAlarm Package: rip.RipDown Raised on class: rip.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a RIP site has an Operational State other than Up, and the Administrative State is Up.		
Raising condition: (('Administrative State' EQUAL 'Up') AND ('Operational State' NOT EQUAL 'Up'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('Administrative State' NOT EQUAL 'Up'))		
Remedial action: The RIP Site is down while it is administratively up. Please check the node e.g, IOM is not shutdown or installed.		

Table 54-83 SaveConfigFailed

Alarm	Attributes	Applicable major release
Name: SaveConfigFailed (105) Type: configurationAlarm Package: sw.SaveConfigFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: fileAccessError	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the admin save command on an NE fails.		
Raising condition: ('Config Save State' EQUAL 'Failure')		
Clearing condition: ('Config Save State' EQUAL 'Success')		
Remedial action: Attempt the admin save command a second time. If the problem persists please contact your Nokia support representative for assistance.		

Table 54-84 ScheduledPollerProblem

Alarm	Attributes	Applicable major release
Name: ScheduledPollerProblem (4386) Type: communicationsAlarm Package: netw.ScheduledPollerProblem Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: scheduledResyncFailed	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM is unable to poll a network object, for example, because of intermittent or no IP connectivity to an NE, incorrect SNMP or Netconf security parameters, or disabled SNMP on the NE.		
Raising condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Failed')		
Clearing condition: ('Scheduled Resync Status' EQUAL 'Scheduled Resync Done')		

Table 54-84 ScheduledPollerProblem (continued)

Alarm	Attributes	Applicable major release
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy to respond to 5620 SAM or c) has SNMP been disabled on the NE. Once the issue has been resolved SAM will automatically re-attempt.		

Table 54-85 ServiceSiteDown

Alarm	Attributes	Applicable major release
Name: ServiceSiteDown (97) Type: serviceAlarm Package: service.ServiceSiteDown Raised on class: service.Site	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: siteDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all SAPs on a site are operationally down, or when the service tunnels for the site are operationally down. For Backhaul Sites, this alarm is raised when one or more Backhaul Adjacencies is operationally down.		
Raising condition: (('Operational State' NOT EQUAL 'Up') AND ('State Cause' NOT EQUAL 'All Spoke SDP Bindings are Standby'))		
Clearing condition: (('Operational State' EQUAL 'Up') OR ('State Cause' EQUAL 'All Spoke SDP Bindings are Standby'))		
Remedial action: The network resources (i.e. physical ports for SAPs or Backhaul Sites, or physical ports/LSP) associated with the service site should be examined to determine if/why they are operationally down. The underlying transport network supporting the site may also be unreliable.		

Table 54-86 SiteManagementVlanConflict

Alarm	Attributes	Applicable major release
Name: SiteManagementVlanConflict (223) Type: configurationAlarm Package: vlan.SiteManagementVlanConflict Raised on class: vlan.Site	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the management VLAN ID is used for another type of service.		
Raising condition: ('managementVlanConflict' EQUAL 'true')		
Clearing condition: ('managementVlanConflict' EQUAL 'false')		
Remedial action: Ensure that the VLAN ID of this Management Service Site is not used on any other type of VLAN Service Site.		

Table 54-87 SiteVlanSubTypeConflict

Alarm	Attributes	Applicable major release
Name: SiteVlanSubTypeConflict (224) Type: configurationAlarm Package: vlan.SiteVlanSubTypeConflict Raised on class: vlan.Site	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: topologyMisconfigured	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when more than one type of VLAN service has the same VLAN ID. The alarm is raised against a site.		
Raising condition: ('vlanSubTypeConflict' EQUAL 'true')		
Clearing condition: ('vlanSubTypeConflict' EQUAL 'false')		
Remedial action: Ensure that only one type of VLAN Service is configured with the VLAN ID used by this Site.		

Table 54-88 StatsRetrieveFailed

Alarm	Attributes	Applicable major release
Name: StatsRetrieveFailed (244) Type: configurationAlarm Package: sw.StatsRetrieveFailed Raised on class: sw.AccountingStatsRetrievalManager	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: fileTransferFailure	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM main or auxiliary server cannot transfer an accounting file from an NE.		
Raising condition: (('Stats Retrieval State' NOT EQUAL 'Success') AND ('Stats Retrieval State' NOT EQUAL 'Not Attempted'))		
Remedial action: Informational - if the alarm persists or is occurring frequently then investigation is required to understand a) why the underlying transport network is unreliable or b) why the NE is too busy or otherwise cannot respond to the 5620 SAM main or auxiliary server.		

Table 54-89 SubscriberSystemNextHopUsageHigh

Alarm	Attributes	Applicable major release
Name: SubscriberSystemNextHopUsageHigh (5157) Type: thresholdCrossed Package: netw.SubscriberSystemNextHopUsageHigh Raised on class: netw.NetworkElement	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit.		
Raising condition: ('IP Next Hop Usage High' EQUAL 'true')		
Clearing condition: ('IP Next Hop Usage High' EQUAL 'false')		

Table 54-89 SubscriberSystemNextHopUsageHigh (continued)

Alarm	Attributes	Applicable major release
Remedial action: The alarm is raised when the IP next-hop usage by subscriber managed routes reaches its high watermark, cleared when it reaches its low watermark again; the watermarks are derived from the limit specified with the property subSysNextHopLimit. There is no immediate effect, but when the usage actually hits the limit, new hosts will not get their managed routes.		

Table 54-90 SubSysChassMemoryUsageHi

Alarm	Attributes	Applicable major release
Name: SubSysChassMemoryUsageHi (5656) Type: thresholdCrossed Package: equipment.SubSysChassMemoryUsageHi Raised on class: equipment.Shelf	Severity: minor Specific problem: Not Applicable Implicitly cleared: true Default probable cause: resourceFull	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This alarm is raised when the memory usage by subscriber management on this system or chassis reaches its high watermark ('true').		
Raising condition: ('Memory Usage High' EQUAL 'True')		
Clearing condition: (('Memory Usage High' EQUAL 'False') OR ('Memory Usage High' EQUAL 'unspecified'))		
Remedial action: The memory usage by subscriber management on this system has reached its high watermark. Please check your memory usage.		

Table 54-91 TemperatureThresholdCrossed

Alarm	Attributes	Applicable major release
Name: TemperatureThresholdCrossed (7) Type: environmentalAlarm Package: equipment.TemperatureThresholdCrossed Raised on class: equipment.Environment	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: equipmentOverheated	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a temperature crosses a threshold.		
Raising condition: ('temperatureThresholdCrossed' EQUAL 'true')		
Clearing condition: ('temperatureThresholdCrossed' EQUAL 'false')		
Remedial action: The NE has detected internal temperatures which are abnormally high. This could be caused by a failed fan unit or one or more dirty fan filters. Replacing the failed unit or filters should resolve the problem. Alternately the environment that the NE is operating in may not be within specifications found in the NE user guides.		

Table 54-92 TlsSiteDown

Alarm	Attributes	Applicable major release
Name: TlsSiteDown (163) Type: ProtocolAlarm Package: layer2.TlsSiteDown Raised on class: layer2.TlsSite	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: protocolDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when MVR is disabled on an NE and a TLS VLAN or MVR VLAN service is provisioned on the NE.		
Raising condition: ('TLS Admin Status' EQUAL 'Disabled')		
Clearing condition: ('TLS Admin Status' EQUAL 'Enabled')		
Remedial action: To clear the alarm, enable TLS Admin Status under the Bridge Instance.		

Table 54-93 TmnxEqPortEtherLoopDetected

Alarm	Attributes	Applicable major release
Name: TmnxEqPortEtherLoopDetected (461) Type: portEtherLoopDetected Package: ethernetequipment. TmnxEqPortEtherLoopDetected Raised on class: ethernetequipment. EthernetPortSpecifics	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: HighBer	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when a device detects a physical loop on an Ethernet port.		
Raising condition: (('Down When Looped Status' EQUAL 'Loop Detected'))		
Clearing condition: (('Down When Looped Status' EQUAL 'No Loop Detected'))		
Remedial action: An Ethernet port has been mis-cabled - please remove the loopback cable on the port.		

Table 54-94 TrapDestinationMisconfigured

Alarm	Attributes	Applicable major release
Name: TrapDestinationMisconfigured (33) Type: configurationAlarm Package: netw.TrapDestinationMisconfigured Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapDestinationMisconfigured Applicable probable causes: • trapDestinationMisconfigured • duplicateTrapLogId	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 5620 SAM cannot be added to the NE's SNMP trap destinations.		
Raising condition: ('isTrapDestinationMisconfigured' EQUAL 'true')		
Clearing condition: ('isTrapDestinationMisconfigured' EQUAL 'false')		

Table 54-94 TrapDestinationMisconfigured (continued)

Alarm	Attributes	Applicable major release
Remedial action: A configuration error has been made which must be corrected. The SNMP trap destination on the NE must be configured to the IP address of the SAM server.		

Table 54-95 TrapReceivingFailure

Alarm	Attributes	Applicable major release
Name: TrapReceivingFailure (1083) Type: communications Package: netw.TrapReceivingFailure Raised on class: netw.NetworkElement	Severity: major Specific problem: Not Applicable Implicitly cleared: false Default probable cause: trapsWillNotBeSent	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: This user-defined alarm is raised when the NE is unable to send traps because the NE configuration is one of the following: - The Management IP Selection is set to Out Of Band Only, the Primary Route Preference is set to In Band, and the Secondary Route Preference is set to None. - The Management IP Selection is set to In Band Only, the Primary Route Preference is set to Out Of Band, and the Secondary Route Preference is set to None.		
Raising condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Only') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Only') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'In Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'In Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'In Band') OR ('Secondary Route Preference' EQUAL 'In Band'))) OR (('Active Management IP' EQUAL 'Out Of Band') AND ('Management IP Selection' EQUAL 'Out Of Band Preferred') AND (('Primary Route Preference' EQUAL 'Out Of Band') OR ('Secondary Route Preference' EQUAL 'Out Of Band'))))		
Remedial action: A configuration error has been made which must be corrected. The configuration error must be corrected per the discussion in the description for this alarm.		

Table 54-96 TrapRoutePreferenceRedundancyMissing

Alarm	Attributes	Applicable major release
Name: TrapRoutePreferenceRedundancyMissing (1084) Type: communications Package: netw. TrapRoutePreferenceRedundancyMissing Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: trapsRedundancyMissing	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The user-defined alarm is raised when NE management redundancy is configured without trap route preference redundancy.		
Raising condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Primary Route Preference' EQUAL 'In Band') AND ('Secondary Route Preference' EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Primary Route Preference' EQUAL 'Out Of Band') AND ('Secondary Route Preference' EQUAL 'None')))		
Clearing condition: ((('Management IP Selection' EQUAL 'In Band Preferred') AND ('Active Management IP' EQUAL 'In Band') AND ('Secondary Route Preference' NOT EQUAL 'None')) OR (('Management IP Selection' EQUAL 'Out Of Band Preferred') AND ('Active Management IP' EQUAL 'Out Of Band') AND ('Secondary Route Preference' NOT EQUAL 'None')))		
Remedial action: A configuration error has been made which must be corrected. The IP address of the standby SAM server must be configured on the NE in question.		

Table 54-97 UnidentifiedNode

Alarm	Attributes	Applicable major release
Name: UnidentifiedNode (1922) Type: communicationsAlarm Package: netw.UnidentifiedNode Raised on class: netw.DiscoveredNode	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unidentifiedNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the node being discovered can not be properly identified.		
Raising condition: ('State' EQUAL 'Pending Identification')		
Clearing condition: ('State' NOT EQUAL 'Pending Identification')		
Remedial action: A configuration error has occurred that must be corrected. The eNodeB does not have a system name. The name can be configured by selecting the alarm, opening the associated properties form for the alarmed object and configuring the system name.		

Table 54-98 UnmanageFailed

Alarm	Attributes	Applicable major release
Name: UnmanageFailed (300) Type: discoveryControlAlarm Package: netw.UnmanageFailed Raised on class: netw.NodeDiscoveryControl	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: unableToDeleteNode	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when an attempt to unmanage an NE fails.		
Raising condition: ('Site State' EQUAL 'Unmanage Failed')		
Clearing condition: ('Site State' NOT EQUAL 'Unmanage Failed')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 54-99 UpgradedBuildVersionMismatch

Alarm	Attributes	Applicable major release
Name: UpgradedBuildVersionMismatch (174) Type: configurationAlarm Package: netw.UpgradedBuildVersionMismatch Raised on class: netw.NetworkElement	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedImageNotBooted	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the software version that an NE reports after a software upgrade does not match the version of the software used for the upgrade.		
Raising condition: ('upgradedBuildVersionMismatch' EQUAL 'true')		
Clearing condition: ('upgradedBuildVersionMismatch' EQUAL 'false')		
Remedial action: Informational - if the alarm persists please contact your Nokia support representative for assistance		

Table 54-100 upgradedCardAlarm

Alarm	Attributes	Applicable major release
Name: upgradedCardAlarm (255) Type: softwareAlarm Package: equipment.upgradedCardAlarm Raised on class: equipment.Card	Severity: warning Specific problem: Not Applicable Implicitly cleared: true Default probable cause: upgradedCard	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the standby CPM is rebooted and operational after a software upgrade. A device resets an IOM automatically after 120 minutes if the IOM is not manually reset after a CPM upgrade.		
Raising condition: ('operationalState' EQUAL 'Upgrade')		
Clearing condition: ('operationalState' EQUAL 'Up')		
Remedial action: Informational - no corrective action required.		

Table 54-101 UplinkDown

Alarm	Attributes	Applicable major release
Name: UplinkDown (11062) Type: virtualSwitchAlarm Package: dctr.UplinkDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsAllDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when all connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '2'))		
Clearing condition: (('uplinkState' NOT EQUAL '2'))		
Remedial action: This alarm is raised when all connections associated to the uplink lost connectivity.		

Table 54-102 UplinkPartiallyDown

Alarm	Attributes	Applicable major release
Name: UplinkPartiallyDown (11063) Type: virtualSwitchAlarm Package: dctr.UplinkPartiallyDown Raised on class: dctr.AbstractUplink	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: ConnectionsDown	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when some connections of the Uplink are down.		
Raising condition: (('uplinkState' EQUAL '3'))		
Clearing condition: (('uplinkState' NOT EQUAL '3'))		
Remedial action: This alarm is raised when a connection of the uplink lost connectivity but at least one connection remains connected.		

Table 54-103 VersionConfigRestoreFailed

Alarm	Attributes	Applicable major release
Name: VersionConfigRestoreFailed (536) Type: configurationAlarm Package: sw.VersionConfigRestoreFailed Raised on class: sw.BackupRestoreManager	Severity: major Specific problem: Not Applicable Implicitly cleared: true Default probable cause: versionMismatch	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the restore procedure on an NE fails because of a mismatch between the backup file set version and the NE software version.		
Raising condition: ('lastNmsVersionRestoreState' EQUAL 'Failure')		
Clearing condition: ('lastNmsVersionRestoreState' EQUAL 'Success')		
Remedial action: The backup files being restored do not match with the version of node software release. Download a new copy of the SW image to the NE. If the problem persists contact your Nokia support representative for assistance.		

Table 54-104 WrongCpaaSoftwareVersion

Alarm	Attributes	Applicable major release
Name: WrongCpaaSoftwareVersion (791) Type: equipmentAlarm Package: netw.WrongCpaaSoftwareVersion Raised on class: netw.NetworkElement	Severity: critical Specific problem: Not Applicable Implicitly cleared: true Default probable cause: wrongCpaaSoftwareVersion	Release: • 6.3.4 • 6.4.2 • 6.4.3
Description: The alarm is raised when the 7701 CPAA software is the wrong version and requires an upgrade.		
Raising condition: (('Software Version' EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Clearing condition: (('Software Version' NOT EQUAL '\"TiMOS-B-3.0.Generic \"') AND ('Chassis Type' EQUAL '7701 CPAA'))		
Remedial action: The SW version of the CPAA must be upgraded to the version compatible with CPAM version.		